Red Hat Enterprise Linux 4

Einführung in die System-Administration

Red Hat Enterprise Linux 4: Einführung in die System-Administration
Copyright © 2005 von Red Hat, Inc.

Red Hat, Inc.

1801 Varsity Drive Raleigh NC 27606-2072 USA Phone: +1 919 754 3700 Phone: 888 733 4281 Fax: +1 919 754 3701 PO Box 13588 Research Triangle Park NC 27709 USA

rhel-isa(DE)-4-Print-RHI (2004-08-25T17:11)
Copyright © 2005 Red Hat, Inc. Das vorliegende Material darf nur unter Einhaltung der in Open Publication License, V1.0 oder neuer dargelegten Geschäftsbedingungen vertrieben werden (die neueste Version ist gegenwärtig unter http://www.opencontent.org/openpub/ verfügbar).
Beträchtlich modifizierte Versionen dieses Dokumentes dürfen nur mit ausdrücklicher Genehmigung des Copyright-Inhabers vertrieben werden.
Der Vertrieb des Werks oder einer Ableitung des Werks in Standardbuchform (Papier) zu kommerziellen Zwecken ist nicht zulässig, sofern dies nicht zuvor durch den Copyright-Inhaber genehmigt wurde.
Red Hat und das Red Hat "Shadow Man" Logo sind eingetragene Warenzeichen oder Warenzeichen der Red Hat, Inc. in den USA und anderen Ländern.
Alle weiteren hier genannten Rechte an Warenzeichen sowie Copyrights liegen bei den jeweiligen Eigentümern.
Der GPG-Code des security@redhat.com Schlüssels lautet:
CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

Inhaltsverzeichnis

Einführung ..... **i**
1. Architektur-spezifische Informationen i
2. Dokumentkonventionen ii
3. Aktivieren Sie Ihr Abonnement iv
3.1. Geben Sie Ihre Red Hat Benutzerkennung und Passwort ein v
3.2. Geben Sie Ihre Abonnementnummer ein v
3.3. Verbinden Sie Ihr System v
4. Es kommt noch mehr vi
4.1. Senden Sie uns Ihr Feedback vi
1. Philosophie der Systemadministration **1**
1.1. Alles automatisieren 1
1.2. Alles dokumentieren 2
1.3. So viel wie möglich kommunizieren 3
1.3.1. Sagen Sie den Benutzern, was Sie machen werden 3
1.3.2. Sagen Sie Benutzern, was Sie gerade machen 4
1.3.3. Sagen Sie den Benutzern, was Sie gemacht haben 5
1.4. Kennen Sie Ihre Ressourcen 6
1.5. Kennen Sie Ihre Benutzer 6
1.6. Kennen Sie Ihren Geschäftsbereich 6
1.7. Sicherheit darf nicht vernachlässigt werden 7
1.7.1. Das Risiko des Social Engineering 7
1.8. Vorausplanen 8
1.9. Erwarten Sie das Unerwartete 8
1.10. Red Hat Enterprise Linux-spezifische Informationen 9
1.10.1. Automatisierung 9
1.10.2. Dokumentation und Kommunikation 10
1.10.3. Sicherheit 10
1.11. Zusätzliche Ressourcen 11
1.11.1. Installierte Dokumentation 11
1.11.2. Nützliche Webseiten 12
1.11.3. Bücher zum Thema 12
2. Ressourcenkontrolle **15**
2.1. Grundlegende Konzepte 15
2.2. System-Leistungskontrolle 15
2.3. Überwachen der Systemkapazität 16
2.4. Was überwachen? 16
2.4.1. Überwachung der CPU-Leistung 17
2.4.2. Überwachung der Bandbreite 18
2.4.3. Überwachung von Speicher 19
2.4.4. Überwachen von Speicherplatz 19
2.5. Red Hat Enterprise Linux-spezifische Informationen 20
2.5.1. `free` 20
2.5.2. `top` 21
2.5.3. `vmstat` 23
2.5.4. Die Sysstat-Suite von Ressourcenüberwachungstools 24
2.5.5. OProfile 28
2.6. Zusätzliche Ressourcen 31
2.6.1. Installierte Dokumentation 31
2.6.2. Nützliche Webseiten 32
2.6.3. Themenbezogene Literatur 32

3. Bandbreite und Prozessleistung 35
3.1. Bandbreite 35
3.1.1. Busse 35
3.1.2. Datenpfade 36
3.1.3. Potentielle Bandbreiten-bezogene Probleme 36
3.1.4. Potenzielle, Bandbreiten-bezogene Lösungen 37
3.1.5. Im Überblick... 38
3.2. Prozessleistung 38
3.2.1. Fakten über Prozessleistung 38
3.2.2. Konsumenten der Prozessleistung 39
3.2.3. Verbessern eines CPU-Engpasses 39
3.3. Red Hat Enterprise Linux-spezifische Information 42
3.3.1. Überwachung von Bandbreite auf Red Hat Enterprise Linux 42
3.3.2. Überwachung der CPU-Nutzung auf Red Hat Enterprise Linux 44
3.4. Zusätzliche Ressourcen 48
3.4.1. Installierte Dokumentation 48
3.4.2. Nützliche Webseiten 49
3.4.3. Bücher zum Thema 49
4. Physikalischer und virtueller Speicher 51
4.1. Zugriffsmuster auf Speicher 51
4.2. Das Speicherspektrum 51
4.2.1. CPU-Register 52
4.2.2. Cache-Speicher 52
4.2.3. Hauptspeicher — RAM 53
4.2.4. Festplatten 54
4.2.5. Offline-Datensicherungsspeicher (Offline-Backup-Speicher) 55
4.3. Grundlegende Konzepte virtuellen Speichers 56
4.3.1. Virtueller Speicher in einfachen Worten 56
4.3.2. Zusatzspeicher — zentraler Grundsatz des virtuellen Speichers 57
4.4. Virtueller Speicher: Die Details 57
4.4.1. Seitenfehler (Page Faults) 58
4.4.2. Die Arbeitsmenge (Working Set) 58
4.4.3. Seitenaustausch (Swapping) 59
4.5. Schlussfolgerungen zur Leistungsfähigkeit bei der Benutzung von virtuellem Speicher 59
4.5.1. Schlimmster Fall in puncto Leistungsfähigkeit 60
4.5.2. Bester Fall in puncto Leistungsfähigkeit 60
4.6. Red Hat Enterprise Linux-spezifische Information 60
4.7. Zusätzliche Ressourcen 63
4.7.1. Installierte Dokumentation 63
4.7.2. Nützliche Webseiten 64
4.7.3. Bücher zum Thema 64
5. Speicher verwalten 67
5.1. Ein Überblick über Speicher-Hardware 67
5.1.1. Disk Platten 67
5.1.2. Daten Schreib-/Lesegerät 67
5.1.3. Zugriffsarme 68
5.2. Konzepte der Speicheradressierung 69
5.2.1. Geometrie-basierte Adressierung 69
5.2.2. Block-basierte Adressierung 71
5.3. Schnittstellen der Massenspeichergeräte 71
5.3.1. Historischer Hintergrund 71
5.3.2. Heutige Industrie-Standard-Schnittstellen 72
5.4. Performance-Merkmale der Festplatte 75
5.4.1. Mechanische/Elektrische Einschränkungen 75
5.4.2. I/O-Lasten und Performance 77

5.5. Den Speicher nutzbar machen ... 78
5.5.1. Partitionen/Slices ... 78
5.5.2. Dateisysteme ... 80
5.5.3. Verzeichnisstruktur ... 82
5.5.4. Speicherzugang ermöglichen ... 83
5.6. Fortgeschrittene Speicher-Technologien ... 83
5.6.1. Netzwerk-zugänglicher Speicher ... 83
5.6.2. RAID-basierter Speicher ... 84
5.6.3. Logical Volume Management (LVM) ... 90
5.7. Tagtägliche Speicherverwaltung ... 91
5.7.1. Freien Speicher überwachen ... 91
5.7.2. Probleme mit Festplattenquoten ... 94
5.7.3. Datei-bezogene Probleme ... 95
5.7.4. Speicher hinzufügen/löschen ... 96
5.8. Weiteres zu Backups... ... 102
5.9. Red Hat Enterprise Linux-spezifische Informationen ... 102
5.9.1. Gerätenamen-Konventionen ... 102
5.9.2. Grundlagen zum Dateisystem ... 105
5.9.3. Dateisysteme mounten ... 107
5.9.4. Netzwerk-zugänglicher Speicher unter Red Hat Enterprise Linux ... 110
5.9.5. Dateisysteme automatisch mit `/etc/fstab` mounten ... 111
5.9.6. Speicher hinzufügen/löschen ... 111
5.9.7. Festplattenquoten implementieren ... 115
5.9.8. RAID-Arrays erstellen ... 119
5.9.9. Tägliche Verwaltung des RAID-Arrays ... 121
5.9.10. Logical Volume Management (LVM) ... 122
5.10. Zusätzliche Ressourcen ... 122
5.10.1. Installierte Dokumentation ... 122
5.10.2. Nützliche Webseiten ... 123
5.10.3. Bücher zum Thema ... 123
6. Verwalten von Benutzer-Accounts und Ressourcen-Zugang ... 125
6.1. Verwalten von Benutzer-Accounts ... 125
6.1.1. Der Benutzername ... 125
6.1.2. Passwörter ... 128
6.1.3. Zugriffskontrolle Information ... 133
6.1.4. Accounts und Ressourcen-Zugang tagtäglich verwalten ... 134
6.2. Verwaltung von Benutzer-Ressourcen ... 136
6.2.1. Wer kann auf gemeinsam genutzte Daten zugreifen ... 136
6.2.2. Wo Benutzer auf gemeinsame Daten zugreifen ... 137
6.2.3. Welche Hemmnisse werden eingesetzt, um den Missbrauch von Ressourcen zu verhindern ... 138
6.3. Red Hat Enterprise Linux-Spezifische Informationen ... 138
6.3.1. Benutzer-Accounts, Gruppen und Berechtigungen ... 139
6.3.2. Dateien, die Benutzer-Accounts und -Gruppen kontrollieren ... 141
6.3.3. Benutzer-Account und Gruppen-Applikationen ... 144
6.4. Zusätzliche Ressourcen ... 146
6.4.1. Installierte Dokumentation ... 146
6.4.2. Nützliche Webseiten ... 147
6.4.3. Darauf bezogenen Literatur ... 147

7. Drucker und Drucken 149
7.1. Druckertypen 149
7.1.1. Erwägungen zum Thema Drucken 149
7.2. Anschlagdrucker 151
7.2.1. Punktmatrixdrucker 151
7.2.2. Typenraddrucker 151
7.2.3. Zeilendrucker 151
7.2.4. Anschlagdrucker Verbrauchsmaterialien 152
7.3. Tintenstrahldrucker 152
7.3.1. Tintenstrahler Verbrauchsmaterialien 152
7.4. Laserdrucker 153
7.4.1. Farblaserdrucker 153
7.4.2. Laserdrucker Verbrauchsmaterialien 153
7.5. Andere Druckerarten 154
7.6. Druckersprachen und Technologien 155
7.7. Vernetzte versus lokale Drucker 155
7.8. Red Hat Enterprise Linux-spezifische Information 156
7.9. Zusätzlich Quellen 157
7.9.1. Installierte Dokumentation 157
7.9.2. Nützliche Websites 158
7.9.3. Themenbezogene Literatur 158
8. Auf das Schlimmste vorbereiten 159
8.1. Arten von Katastrophen 159
8.1.1. Hardware-Ausfälle 159
8.1.2. Software-Ausfälle 165
8.1.3. Ausfälle der Umgebung 167
8.1.4. Menschliches Versagen 174
8.2. Backups 178
8.2.1. Verschiedene Daten: Verschiedene Backup-Ansprüche 178
8.2.2. Backup-Software - Kaufen versus Erstellen 180
8.2.3. Arten von Backups 181
8.2.4. Backup-Medien 182
8.2.5. Lagern von Backups 184
8.2.6. Wiederherstellung 184
8.3. Wiederherstellung nach einem Disaster 185
8.3.1. Erstellen, Testen und Implementieren eines Wiederherstellungsplans nach Katastrophen 186
8.3.2. Backup-Orte: Kalt, Warm und Heiß 187
8.3.3. Hardware- und Softwareverfügbarkeit 188
8.3.4. Backup-Verfügbarkeit 188
8.3.5. Netzwerverbindung zum Backup-Ort 188
8.3.6. Belegschaft des Backup-Ortes 188
8.3.7. Rückkehr zum Normalzustand 189
8.4. Red Hat Enterprise Linux-spezifische Informationen 189
8.4.1. Software-Support 189
8.4.2. Backup-Technologien 190
8.5. Zusätzliche Ressourcen 193
8.5.1. Installierte Dokumentation 193
8.5.2. Nützliche Webseiten 193
8.5.3. Bücher zum Thema 194
Stichwortverzeichnis 195
Colophon 203

Einführung

Willkommen zu *Red Hat Enterprise Linux Einführung in die System-Administration*.

Red Hat Enterprise Linux Einführung in die System-Administration beinhaltet Informationen zur Einführung von neuen Red Hat Enterprise Linux System Administratoren. Es lehrt *nicht* wie bestimmte Aufgaben unter Red Hat Enterprise Linux erfüllt werden können; es vermittelt Ihnen hingegen Hintergrundwissen, welches sich erfahrene Systemadministratoren über Jahre hinweg angeeignet haben.

In diesem Handbuch wird davon ausgegangen, dass Sie begrenzte Erfahrung als Linux-Benutzer besitzen, jedoch keinerlei Erfahrung als Linux System Administrator. Wenn Sie ein kompletter Linux-Neueinsteiger (und speziell Red Hat Enterprise Linux) sind, so sollten Sie zuallererst mit einem Linux-Einführungsbuch beginnen.

Jedes Kapitel in *Red Hat Enterprise Linux Einführung in die System-Administration* besitzt folgende Struktur:

- Generisches Überblicksmaterial — Dieser Abschnitt behandelt das jeweilige Thema des Abschnittes, ohne dabei ins Detail zu gehen in Bezug auf ein spezifisches Betriebssystem, Technologie oder Methodik.
- Red Hat Enterprise Linux-spezifisches Material — Dieser Abschnitt behandelt Aspekte des Themas in generellem Bezug auf Linux und spezieller Hinsicht auf Red Hat Enterprise Linux.
- Zusätzliche Ressourcen zur themengerechten Weiterbildung — Dieser Abschnitt enthält Verweise auf andere Red Hat Enterprise Linux Handbücher, hilfreiche Webseiten und Bücher, die Informationen zum Thema enthalten.

Durch die Anwendung einer gleichbleibenden Struktur, kann *Red Hat Enterprise Linux Einführung in die System-Administration* einfacher auf verschiedenen Arten gelesen werden, über die der Leser selbst entscheidet. Zum Beispiel könnte ein erfahrener Systemadministrator mit geringer Red Hat Enterprise Linux-Erfahrung lediglich die Abschnitte durchgehen, die sich speziell mit Red Hat Enterprise Linux befassen. Ein neuer Systemadministrator hingegen könnte damit beginnen, lediglich die Abschnitte zu lesen, die einen allgemeinen Überblick vermitteln und später die Red Hat Enterprise Linux-spezifischen Abschnitte für ein tiefgreifenderes Wissen.

Zum Thema fundamentalerer Ressourcen, stellt *Red Hat Enterprise Linux Handbuch zur System-Administration* eine ausgezeichnete Quelle zur Wissensbildung bezüglich der Ausführung spezifischer Aufgaben in einer Red Hat Enterprise Linux-Umgebung dar. Administratoren, die noch tiefgreifendere, sachbezogene Informationen benötigen, sollten sich auf das *Red Hat Enterprise Linux Referenzhandbuch* beziehen.

HTML-, PDF- und RPM-Versionen der Handbücher sind auf der Red Hat Enterprise Linux Dokumentations-CD und Online unter http://www.redhat.com/docs/ erhältlich.

Anmerkung

Obwohl dieses Handbuch die neuesten Informationen enthält, lesen Sie die *Red Hat Enterprise Linux Release-Notes* für weitere Information, die zum Druck dieses Handbuchs noch nicht vorlagen. Diese können auf der Red Hat Enterprise Linux CD #1 und Online unter http://www.redhat.com/docs/ gefunden werden.

1. Architektur-spezifische Informationen

Sofern nicht anders angegeben, bezieht sich jegliche Information in diesem Handbuch nur auf den x86-Prozessor und auf Prozessoren mit Intel® Extended Memory 64 Technology (Intel® EM64T)

und AMD64 Technologien. Für Architektur-spezifische Informationen siehe das *Red Hat Enterprise Linux Installationshandbuch* für Ihre respektive Architektur.

2. Dokumentkonventionen

Beim Lesen dieses Handbuchs werden Sie feststellen, dass bestimmte Wörter in verschiedenen Fonts, Schriftbildern, Größen usw. dargestellt sind. Diese Unterscheidung folgt einer bestimmten Ordnung: bestimmte Wörter werden auf die gleiche Weise dargestellt, um darauf hinzuweisen, dass sie zu einer bestimmten Kategorie gehören. Typen von Begriffen, die auf diese Art dargestellt werden, schließen folgende Begriffe ein:

`Befehl`

Linux-Befehle (sowie Befehle anderer Betriebssysteme, sofern verwendet) werden auf diese Weise dargestellt. Diese Darstellungsart weist darauf hin, dass Sie das Wort oder den Satz in die Befehlszeile eingeben und die [Enter-Taste] drücken können, um den entsprechenden Befehl auszuführen. Gelegentlich enthält ein Befehl Wörter, die eigentlich auf eine andere Weise dargestellt werden würden (beispielsweise Dateinamen). In einem solchen Fall werden sie als Teil des Befehls betrachtet und der gesamte Satz wird als Befehl dargestellt. Beispiel:

Verwenden Sie den Befehl `cat testfile`, um den Inhalt einer Datei mit dem Namen `testfile` in einem aktuellen Verzeichnis anzeigen zu lassen.

`Dateiname`

Datei- und Verzeichnisnamen sowie die Namen von Pfaden und RPM-Paketen werden auf diese Weise dargestellt, was bedeutet, dass eine bestimmte Datei oder ein bestimmtes Verzeichnis mit diesem Namen in Ihrem System vorhanden ist. Beispiele:

Die Datei `.bashrc` in Ihrem Home-Verzeichnis enthält Bash-Shell Definitionen und Aliase für Ihren Gebrauch.

Die Datei `/etc/fstab` enthält Informationen über verschiedene Systemgeräte und Dateisysteme.

Installieren Sie den `webalizer` RPM, wenn Sie ein Analyseprogramm für eine Webserver-Protokolldatei verwenden möchten.

Applikation

Diese Darstellungsart weist darauf hin, dass es sich bei diesem Programm um eine Endbenutzer-Anwendung handelt (im Gegensatz zur System-Software). Beispiel:

Verwenden Sie **Mozilla**, um im Web zu browsen.

[Taste]

Die Tasten der Tastatur werden auf diese Weise dargestellt. Beispiel:

Um die [Tab]-Vervollständigung zu verwenden, geben Sie einen Buchstaben ein und drücken Sie anschließend die Taste [Tab]. Auf diese Weise wird die Liste der Dateien im Verzeichnis angezeigt, die mit diesem Buchstaben beginnen.

[Tasten]-[Kombination]

Eine Tastenkombination wird auf diese Art und Weise dargestellt.

Mit der Tastenkombination [Strg]-[Alt]-[Rücktaste] beenden Sie Ihre grafische Sitzung und kehren zum grafischen Anmeldebildschirm oder zur Konsole zurück.

Text in der GUI-Schnittstelle

Überschriften, Worte oder Sätze, die Sie auf dem GUI-Schnittstellenbildschirm oder in Window finden, werden in diesem Stil wiedergegeben. Wenn Sie daher einen Text in diesem Stil finden, soll dieser einen bestimmten GUI-Bildschirm oder ein Element eines GUI-Bildschirms (z.B. ein Text, der sich auf ein Kontrollkästchen oder auf ein Feld bezieht) identifizieren. Beispiel:

Wählen Sie das Kontrollkästchen **Passwort erforderlich**, wenn Ihr Bildschirmschoner passwortgeschützt sein soll.

Erste Menüstufe auf einem GUI-Bildschirm oder in einem Fenster

Wenn ein Wort auf diese Art und Weise dargestellt ist, zeigt dies an, dass es sich hierbei um den Anfang eines Pulldown-Menüs handelt. Beim Klicken auf das Wort auf dem GUI-Bildschirm erscheint der Rest des Menüs. Zum Beispiel:

Unter **Datei** auf dem GNOME-Terminal sehen Sie die Option **Neuer Tab**, mit dem Sie mehrere Shell Prompts im gleichen Fenster öffnen können.

Wenn Sie eine Befehlsreihe aus einem GUI-Menü eingeben wollen, wird diese entsprechend dem folgenden Beispiel angezeigt:

Indem Sie **Hauptmenü** (im Panel) => **Programmieren** => **Emacs** wählen, starten Sie den Texteditor **Emacs**.

Schaltfläche auf einem GUI-Bildschirm oder in einem Fenster

Diese Darstellungsweise zeigt an, dass man den betreffenden Text auf der Schaltfläche eines GUI-Bildschirms finden kann. Zum Beispiel:

Indem Sie auf die Schaltfläche **Zurück** klicken, kehren Sie auf die Website zurück, die Sie zuletzt angesehen haben.

`Computerausgabe`

Text, der in diesem Stil dargestellt wird, ist Text, der in einem Shell-Prompt ausgegeben wird, wie Fehlermeldungen und Antworten auf bestimmte Befehle. Zum Beispiel:

Durch Eingabe von `ls` erscheint der Inhalt eines Verzeichnisses. Zum Beispiel:

```
Desktop                about.html       logs          paulwesterberg.png
Mail                   backupfiles      mail          reports
```

Die Ausgabe, die als Antwort auf den Befehl erscheint (in diesem Fall der Inhalt des Verzeichnisses), wird auf diese Art und Weise dargestellt.

`Prompt`

Ein Prompt wird auf diese Art und Weise dargestellt, wenn der Computer Ihnen mitteilen will, dass Sie nun eine Eingabe tätigen können. Beispiele:

```
$
```

```
#
```

```
[stephen@maturin stephen]$
```

```
leopard login:
```

`Benutzereingabe`

Ein Text wird auf diese Art und Weise dargestellt, wenn er vom Benutzer entweder in die Befehlszeile oder in die Textbox auf einem GUI-Bildschirm eingegeben werden soll. Im folgenden Beispiel wird **`text`** in diesem Stil angezeigt:

Mit dem Befehl **`text`** am Prompt `boot:` booten Sie Ihr System in das textbasierte Installationsprogramm.

replaceable

Text, der für Beispiele benutzt wird und dafür vorgesehen ist, durch Daten ersetzt zu werden, wird in diesem Stil dargestellt. Im folgenden Beispiel ist <*version-number*> in dieser Form dargestellt.

Das Verzeichnis für den Kernel-Source ist `/usr/src/`<*version-number*>`/`, wobei <*version-number*> die Version des installierten Kernel ist.

Zusätzlich machen wir Sie mit Hilfe von bestimmten Strategien auf bestimmte Informationen aufmerksam. Entsprechend dem Wichtigkeitsgrad, das die jeweilige Information für Ihr System hat, sind diese Items entweder als Anmerkung, Hinweis oder Warnung gekennzeichnet. Zum Beispiel:

Anmerkung

Beachten Sie, dass Linux ein fallspezifisches System ist. In anderen Worten bedeutet dies, dass Rose nicht das gleiche ist wie ROSE und dies auch nicht das gleiche wie rOsE.

Tipp

Das Verzeichnis `/usr/share/doc/` enthält zusätzliche Dokumentationen für im System installierte Pakete.

Wichtig

Wenn Sie die DHCP Konfigurationsdatei bearbeiten, werden die Änderungen erst wirksam, wenn Sie den DHCP-Daemon neu gestartet haben.

Achtung

Führen Sie keine alltäglichen Aufgaben als root aus — verwenden Sie hierzu ausser für den Fall, dass Sie einen root-Account für Ihre Systemverwaltung benutzen, einen regulären Benutzeraccount.

Warnung

Seien Sie vorsichtig und entfernen Sie lediglich die notwendigen Red Hat Enterprise Linux Partitionen. Das Entfernen anderer Partitionen könnte zu Datenverlusten oder zur Korruption der Systemumgebung führen.

3. Aktivieren Sie Ihr Abonnement

Bevor Sie auf Service- und Softwarewartungs-Information sowie auch der Support-Dokumentation zugreifen können, welche in Ihrem Abonnement inkludiert ist, müssen Sie Ihr Abonnement aktivieren, indem Sie sich bei Red Hat registrieren. Die Registrierung setzt sich aus folgenden simplen Schritten zusammen:

- Geben Sie Ihre Red Hat Benutzerkennung und Passwort ein
- Geben Sie Ihre Abonnementnummer ein
- Verbinden Sie Ihr System

Wenn Sie das erste mal Ihre Red Hat Enterprise Linux-Installation booten, werden Sie aufgefordert sich bei Red Hat mittels **Setup Agent** zu registrieren. Indem Sie einfach den Eingabeaufforderungen im **Setup Agent** folgen, können Sie sämtliche Registrierungsschritte vervollständigen und Ihr Abonnement aktivieren.

Wenn Sie die Registrierung mittels **Setup Agent** (Netzwerkzugang ist erforderlich) nicht durchführen können, so können Sie alternativ dazu auch den Red Hat Registrierungsprozess online unter http://www.redhat.com/register/ verwenden.

3.1. Geben Sie Ihre Red Hat Benutzerkennung und Passwort ein

Sollten Sie kein bestehendes Red Hat Login besitzen, so können Sie Ihre Benutzerkennung und Passwort kreieren, sobald Sie dazu im **Setup Agent** aufgefordert werden oder auch online unter:

```
https://www.redhat.com/apps/activate/newlogin.html
```

Ein Red Hat Login ermöglicht Ihnen Zugang zu:

- Software Updates, Errata und Maintenance via Red Hat Network
- Red Hat Ressourcen auf 'Technischer Support'-Ebene, Dokumentation und Wissensdatenbank

Sollten Sie Ihr Red Hat Login vergessen haben, so können Sie nach Ihrem Red Hat Login auch online suchen:

```
https://rhn.redhat.com/help/forgot_password.pxt
```

3.2. Geben Sie Ihre Abonnementnummer ein

Ihre Abonnementnummer befindet sich im Paket mit Ihrer Bestellung. Sollte sich in Ihrem Paket keine Abonnementnummer befinden, so bedeutet dies, dass Ihr Abonnement für Sie bereits aktiviert worden ist und Sie diesen Schritt überspringen können.

Sie können Ihre Abonnementnummer eingeben, wenn Sie dazu im **Setup Agent** aufgefordert werden oder Sie besuchen http://www.redhat.com/register/.

3.3. Verbinden Sie Ihr System

Der Red Hat Network Registrierungs-Client hilft Ihnen bei Ihrer Systemverbindung, sodass Sie schlussendlich Updates erhalten und mit dem System-Management beginnen können.

1. Während der Registrierung im **Setup Agent** — Ticken Sie die Optionen **Hardware-Information senden** und **System-Paketliste senden**, sobald Sie dazu die Eingabeaufforderung erhalten.

2. Nachdem die Registrierung im **Setup Agent** abgeschlossen wurde — Vom **Hauptmenü** aus gehen Sie zu **System-Tools** und wählen dort **Red Hat Network** aus.
3. Nachdem die Registrierung im **Setup Agent** abgeschlossen wurde — Geben Sie folgenden Befehl von der Befehlszeile als root-Benutzer ein:
   - `/usr/bin/up2date --register`

4. Es kommt noch mehr

Red Hat Enterprise Linux Einführung in die System-Administration ist ein Teil von Red Hats wachsendem Engagement, Red Hat Enterprise Linux-Benutzern nützlichen und zeitgerechten Support bieten zu können. Sobald neue Versionen von Red Hat Enterprise Linux freigegeben werden, bemühen wir uns sehr, eine neue sowie auch verbesserte Dokumentation für Sie zur Verfügung zu stellen.

4.1. Senden Sie uns Ihr Feedback

Wenn Sie einen Tippfehler in *Red Hat Enterprise Linux Einführung in die System-Administration* bemerken oder Sie sich Gedanken darüber gemacht haben, wie man dieses Handbuch verbessern könnte, so würden wir uns sehr freuen von Ihnen dahingehend zu hören. Bitte reichen Sie einen Report in Bugzilla ein (http://bugzilla.redhat.com/bugzilla) zum Komponenten `rhel-isa`.

Vergessen Sie dabei bitte nicht die Kennung des Handbuches anzugeben:

```
rhel-isa(DE)-4-Print-RHI (2004-08-25T17:11)
```

Wenn Sie diese Kennung des Handbuches erwähnen, dann wissen wir genau welche Version des Handbuches Sie besitzen.

Wenn Sie einen Vorschlag zur Verbesserung der Dokumentation an der Hand haben, dann versuchen Sie bitte so spezifisch als möglich zu sein. Wenn Sie einen Fehler gefunden haben, dann inkludieren Sie bitte die Nummer des Abschnittes und ein wenig des Umgebungstextes, sodass es für uns leichter auffindbar ist.

Kapitel 1.

Philosophie der Systemadministration

Auch wenn die Details in der Arbeitsbeschreibung eines Systemadministrators sich von Plattform zu Plattform ändern, gibt es tieferliegende Dinge, die sich nicht ändern. Diese Dinge machen die Philosophie der Systemadministration aus.

Diese Dinge sind:

- Alles automatisieren
- Alles dokumentieren
- So viel wie möglich kommunizieren
- Ihre Ressourcen kennen
- Ihre Benutzer kennen
- Ihren Geschäftsbereich kennen
- Sicherheit darf kein nachträglicher Gedanke sein
- Vorausplanen
- Erwarte das Unerwartete

Die folgenden Abschnitte beschreiben jedes dieser Themen in größerem Detail.

1.1. Alles automatisieren

Die meisten Systemadministratoren sind zahlenmäßig unterlegen — in Bezug auf Benutzer, deren Systeme oder beidem. Auf viele Arten ist die Automatisierung der einzige Weg mitzuhalten. Im Allgemeinen sollte alles, was mehr als einmal gemacht werden muss, als Kandidat für eine Automatisierung angesehen werden.

Hier einige häufig automatisierte Aufgaben:

- Prüfen auf freien Festplattenplatz und Reporterstellung
- Backups
- Datensammlung zur Systemleistung
- Wartung von Benutzeraccounts (Erstellung, Löschen etc.)
- Unternehmensspezifische Funktionen (neue Daten auf Webserver verschieben, monatliche/vierteljährliche/jährliche Reporte erstellen)

Diese Liste ist keineswegs vollständig; die von Systemadministratoren automatisierten Funktionen sind nur beschränkt durch die Bereitschaft des Systemadministrators, die nötigen Skripte zu schreiben. In diesem Fall ist Bequemlichkeit (und damit den Computer die eher lästigen Sachen machen zu lassen) eine gute Eigenschaft.

Automatisierung gibt den Benutzern den Extra-Vorteil einer besseren Vorhersehbarkeit und Konsistenz des Services.

Tipp

Denken Sie daran, dass wenn Sie eine Aufgabe haben, die automatisiert werden soll, Sie wahrscheinlich nicht der erste Systemadministrator sind, der dies möchte. Hier können dann die Vorteile von Open Source Software so richtig glänzen — Sie können eventuell die Arbeit von Anderen nutzen, um einen Prozess zu automatisieren, der bisher sehr viel Ihrer Zeit in Anspruch genommen hat. Stellen Sie also grundsätzlich sicher, dass Sie erst einmal im Internet suchen, bevor Sie irgendetwas Komplexeres als ein kleines Perl-Skript schreiben.

1.2. Alles dokumentieren

Vor der Auswahl stehend, einen neuen Server zu installieren oder ein Dokument über die Erstellung von Systembackups zu schreiben, wählen die meisten Systemadministratoren mit Sicherheit das Installieren des Servers. Während dies nicht unbedingt ungewöhnlich ist, *müssen* Sie jedoch alles das dokumentiern, was von Ihnen getan wird. Viele Systemadministratoren zögern die nötige Dokumentation aus einer Reihe von Gründen hinaus:

"Ich mach das später."

Leider ist dies meistens nicht der Fall. Selbst wenn ein Systemadministrator dies ernst meint, ist jedoch die Natur des Jobs meistens zu chaotisch, um irgendetwas "später" zu erledigen. Noch schlimmer, je länger man die Aufgabe herauszögert, desto mehr wird vergessen, was zu einem weniger detaillierten (und daher auch weniger hilfreichen) Dokument führt.

"Warum aufschreiben? Ich werd es schon nicht vergessen."

Wenn Sie nicht zufällig ein photografisches Gedächtnis haben, ist die Chance, dass Sie sich genau an alles erinnern, relativ gering. Oder noch schlimmer; Sie erinnern sich nur an die Hälfte und merken nicht, dass Sie einen wesentlichen Teil vergessen haben. Meist führt dies zu enormer Zeitverschwendung, wenn Sie nämlich entweder versuchen, das Vergessene neu zu lernen oder Reparaturen durchführen müssen, weil Sie durch Ihr Halbwissen etwas kaputt gemacht haben.

"Wenn ich es nur in meinem Kopf habe, können sie mich nicht so einfach entlassen — mein Arbeitsplatz ist somit sicher!"

Während dies vielleicht eine Zeit lang funktioniert, führt dies zwangsläufig zu weniger — nicht mehr — Job-Sicherheit. Überlegen Sie sich einmal, was bei einem Notfall passiert. Sie sind vielleicht nicht da; Ihre Dokumentation jedoch rettet die Situation, weil jemand anderes das Problem in Ihrer Abwesenheit dadurch lösen kann. Und vergessen Sie niemals, dass Notfälle immer dann auftreten, wenn das Management gerade genau hinsieht. In diesen Fällen ist es besser, dass Ihre Dokumentation Teil der Lösung ist und nicht Ihre Abwesenheit Teil des Problems.

Zusätzlich dazu, wenn Sie Teil eines kleinen, jedoch wachsenden Unternehmens sind, besteht irgendwann vielleicht der Bedarf an einem zweiten Systemadministrator. Wie kann dieser jedoch lernen, wenn sich alles in Ihrem Kopf befindet? Das Versäumen der Dokumentation kann Sie auch so unersetzlich machen, dass Sie sich damit jegliche Aufstiegschancen im Unternehmen verbauen. Sie könnten dann z.B. für die Person arbeiten, die eingestellt wurde, um Ihnen zu helfen.

Hoffentlich sind Sie jetzt von den Vorteilen der Systemdokumentation überzeugt. Dies bringt uns zur nächsten Frage: Was sollten Sie dokumentieren? Hier eine kleine Liste:

Richtlinien

Richtlinien sind dazu geschrieben, die Beziehung zwischen Ihnen und den Benutzern klar darzulegen und in Form zu fassen. Dies gibt dem Benutzer klar vor, wie deren Anfragen nach

Ressourcen und/oder Unterstützung behandelt werden. Die Art, wie diese Richtlinien an die Community weitergeben werden, ist von Unternehmen zu Unternehmen unterschiedlich.

Prozesse

Prozesse sind Schritt-für-Schritt Abfolgen von Aktionen, die durchgeführt werden müssen, um eine bestimmte Aufgabe zu erledigen. Zu dokumentierende Prozesse sind z.B. Backup-Prozesse, Benutzeraccount-Prozesse, Problem-Reporterstellungs-Prozesse usw.. Wie bei der Automatisierung gilt auch für Prozesse: wird ein Prozess mehr als einmal ausgeführt, so ist es sinnvoll, diesen zu dokumentieren.

Änderungen

Ein großer Teil der Arbeit eines Systemadministrators bezieht sich auf das Durchführen von Änderungen — das Konfigurieren von Systemen für die bestmögliche Leistung, das Ändern von Skripten, das Modifizieren von Konfigurationsdateien, usw.. Alle diese Änderungen sollten dokumentiert werden. Ansonsten werden Sie in Zukunft vielleicht von den Änderungen verwirrt, die Sie ein paar Monate zuvor durchgeführt haben.

Einige Unternehmen verwenden komplexere Methoden für das Verzeichnen von Änderungen, aber in den meisten Fällen ist eine einfache Änderungsübersicht am Anfang einer modifizierten Datei alles, was nötig ist. Jeder Eintrag in dem Änderungsüberblick sollte zumindest folgendes enthalten:

- Den Namen oder die Initialen derjenigen Person, die die Änderungen durchführt
- Das Datum der Änderung
- Der Grund für die Änderung

Dies resultiert in kurzen, jedoch sinnvollen Angaben:

ECB, 12-Juni-2002 — Aktualisierter Eintrag für neuen Drucker für die Buchhaltungsabteilung (um die Fähigkeit des Ersatzdruckers, Duplex zu drucken, zu unterstützen)

1.3. So viel wie möglich kommunizieren

Wenn es um Benutzer geht, können Sie niemals zu viel kommunizieren. Seien Sie sich bewusst, dass die winzigen Systemänderungen, die für Sie fast unmerklich erscheinen, vielleicht jemanden in einer anderen Abteilung völlig verwirren können.

Die Art und Weise, auf die Sie mit den Benutzern kommunizieren, unterscheidet sich von Unternehmen zu Unternehmen. Einige Unternehmen verwenden E-Mail, andere eine interne Webseite. Wieder andere verlassen sich vielleicht auf Usenet oder IRC. Für manche ist vielleicht ein Blatt Papier an einem Mitteilungsbrett in der Gemeinschaftsküche praktikabel. Egal wie, verwenden Sie die Methode, die am besten in Ihrem Unternehmen funktioniert.

Im allgemeinen wird empfohlen, dem folgenden Ansatz, der für das Schreiben von Zeitungsartikeln verwendet wird, zu folgen:

1. Sagen Sie den Benutzern, was Sie machen werden
2. Sagen Sie den Benutzern, was Sie gerade machen
3. Sagen Sie den Benutzern, was Sie gemacht haben

Im folgenden Abschnitt werden diese Schritte eingehender beschrieben.

1.3.1. Sagen Sie den Benutzern, was Sie machen werden

Stellen Sie sicher, dass Sie den Benutzern genügend Warnung vor irgendwelchen Änderungen geben. Die eigentliche Frist hängt davon ab, was genau durchgeführt werden soll (das Aktualisieren eines Betriebssystems erfordert mehr Vorwarnung als das Ändern des Bildschirmhintergrunds)

Als absolutes Minimum sollten Sie beschreiben:

- Die Art der Änderung
- Wann die Änderung durchgeführt wird
- Warum dies durchgeführt wird
- Wielange dies dauern wird
- Die Auswirkungen (wenn überhaupt), die aufgrund der Änderungen zu erwarten sind
- Kontaktinformationen, sollten Fragen oder Bedenken auftreten

Hier eine hypothetische Situation. Die Finanzabteilung hatte Probleme mit einem langsamen Datenbankserver. Sie fahren den Server herunter, aktualisieren das CPU-Modul und booten neu. Sobald dies durchgeführt ist, verschieben Sie die Datenbank auf einen schnelleren, RAID-basierten Speicher. Hier ist ein Beispiel für das Mitteilen dieser Situation:

System-Downtime geplant für Freitag Nacht

> Diesen Freitag ab 18.00 Uhr (17.00 Uhr für unsere Geschäftsstellen in London) stehen alle Finanz-Applikationen für einen Zeitraum von vier Stunden nicht zur Verfügung.
>
> Innerhalb diesen Zeitraums werden Änderungen an der Hardware und Software auf dem Finanz-Datenbank-Server durchgeführt. Diese Änderungen sollten die Zeit für das Ausführen der Kreditoren- und Debitoren-Applikationen und Bilanzen erheblich beschleunigen.
>
> Abgesehen von den Änderungen in der Runtime sollten keine weiteren Änderungen festgestellt werden. Diejenigen von Ihnen, die eigene SQL-Queries erstellt haben, sollten sich jedoch bewusst sein, dass das Layout einiger Indexe geändert wird. Dies wird im Firmen-Intranet auf der Finanzseite dokumentiert.
>
> Haben Sie Fragen, Kommentare oder Bedenken, dann kontaktieren Sie bitte die Systemadministration unter Durchwahl 4321.

Einige Punkte sollten beachtet werden:

- Geben Sie Startzeit und Dauer einer Downtime als Teil der Änderungen effektiv bekannt.
- Stellen Sie sicher, dass der Zeitpunkt der Änderung so bekanntgegeben wird, dass dies für *alle* Benutzer sinnvoll ist, egal wo diese sich gerade befinden.
- Verwenden Sie Begriffe, die jeder verstehen kann. Die betroffenen Kollegen interessiert höchstwahrscheinlich nicht, dass das neue CPU-Modul 2 GHz und doppelt soviel L2-Cache hat oder das die Datenbank auf einem RAID 5 Logischem Volumen gespeichert wird.

1.3.2. Sagen Sie Benutzern, was Sie gerade machen

Dieser Schritt ist hauptsächlich eine kurzfristige Warnung vor der direkt bevorstehenden Änderung; die Mitteilung sollte kurz die erste Nachricht zusammenfassen und die bevorstehende Änderung stärker hervorheben ("Die Systemaktualisierung findet HEUTE NACHT statt"). An dieser Stelle können Sie auch öffentlich alle Fragen, die eventuell eingegangen sind, beantworten.

Als Fortsetzung unseres hypothetischen Beispiels hier eine mögliche kurzfristige Warnung:

System-Downtime *heute Nacht*

Erinnerung: Die am letzten Montag angekündigte System-Downtime wird wie geplant um 18.00 Uhr durchgeführt (17.00 für die Geschäftsstelle in London). Die ursprüngliche Ankündigung befindet sich im Firmenintranet auf der Seite der Systemadministrationen.

Mehrere Kollegen haben angefragt, ob sie heute früher Feierabend machen sollen, um sicherzustellen, dass deren Arbeit vor der Downtime gesichert wird. Dies ist nicht nötig, da die Aktualisierungen die Arbeit auf Personal Workstations nicht beeinflussen.

Denken Sie daran, dass für diejenigen, die ihre eigenen SQL-Queries geschrieben haben, sich das Layout einiger Indexe ändert. Dies wird auf der Finanzseite im Firmenintranet dokumentiert.

Die Benutzer wurden gewarnt; Sie können jetzt die eigentliche Arbeit ausführen.

1.3.3. Sagen Sie den Benutzern, was Sie gemacht haben

Nachdem die Änderungen ausgeführt wurden, *müssen* Sie Ihren Benutzern mitteilen, was Sie gemacht haben. Dies sollte wiederum eine Zusammenfassung der vorhergehenden Nachrichten sein (höchstwahrscheinlich gibt es ein paar Leute, die diese nicht gelesen haben.)[1]

Es gibt jedoch einen wichtigen Zusatz, den Sie hinzufügen müssen. Es ist wichtig, dass Sie den Benutzern den aktuellen Zustand mitteilen. Lief die Aktualisierung nicht so wie geplant? Konnte der neue Server nur die Systeme in Engineering versorgen und nicht die in Finanzen? Diese Art von Problemen müssen hier angesprochen werden.

Unterscheidet sich der aktuelle Status von dem vorhergesagten Status, sollten Sie dies hervorheben und beschreiben, was zum Erreichen des eigentlichen Ziels durchgeführt wird.

In dieser hypothetischen Situation traten während der Downtime Probleme auf. Das neue CPU-Modul funktionierte nicht, ein Anruf beim Hersteller zeigte, dass für diese Upgrade eine spezielle Version des Moduls benötigt wird. Auf der positiven Seite verlief die Migration der Datenbank zum RAID-Volume gut (auch wenn dies etwas länger als geplant dauerte, aufgrund der Probleme mit dem CPU-Modul).

Hier eine Beispiel-Ankündigung:

System-Downtime abgeschlossen

Die für letzten Freitag geplante System-Downtime (siehe Webseite der Systemadministration im Firmenintranet) wurde abgeschlossen. Leider verhinderten Probleme mit der Hardware das Ausführen einer Aufgabe. Aufgrund dessen dauerten die anderen Aufgaben länger als die eigentlich geplanten vier Stunden. Alle Systeme liefen wieder wie geplant um Mitternacht (23.00 Uhr in London).

Aufgrund der weiterhin bestehenden Hardware-Probleme ist die Leistung der Debitoren- und Kreditoren-Applikationen sowie die Bilanzfunktion leicht verbessert, jedoch nicht im geplanten Ausmaß. Eine zweite Downtime ist geplant, sobald alle Probleme, die die bisherige Ausführung der Aufgaben verhindert haben, gelöst wurden.

Bitte beachten Sie, dass die Downtime einige Datenbank-Indexe geändert hat; Diejenigen, die ihre eigenen SQL-Queries geschrieben haben, sollten die Finanzseiten im Firmenintranet prüfen.

Sollten Sie Fragen haben, kontaktieren Sie bitte die Systemadministration unter Durchwahl 4321.

Durch diese Informationen erhalten die Benutzer genügend Hintergrundwissen, um deren Arbeit fortzusetzen und zu verstehen, inwieweit sie von den Änderungen betroffen sind.

---

1. Stellen Sie sicher, dass Sie die Nachricht so schnell wie möglich nach durchgeführter Änderung senden. Auf jeden Fall noch *bevor* Sie nach Hause fahren. Sobald Sie nämlich das Büro verlassen haben, ist es viel zu einfach, dies zu vergessen und Sie lassen damit die Benutzer im Dunkeln, ob diese das System benutzen können oder nicht.

1.4. Kennen Sie Ihre Ressourcen

Systemadministration ist im Wesentlichen das Verteilen verfügbarer Ressourcen auf die Mitarbeiter und Programme, die diese Ressourcen verwenden. Aus diesem Grund ist Ihre Karriere als Systemadministrator eher kurz und stressig, solange Sie nicht voll und ganz verstehen, welche Ressourcen Ihnen zur Verfügung stehen.

Einige der Ressourcen scheinen ziemlich offensichtlich:

- Systemressourcen, wie zum Beispiel verfügbare Prozessorleistung, Speicher und Festplattenplatz
- Netzwerk-Bandweite
- Verfügbares IT-Budget

Einige sind nicht ganz so offensichtlich:

- Die Dienste des Betriebspersonals, anderer Systemadministratoren oder auch der Verwaltungsangestellten
- Zeit (meistens sehr wichtig, wenn diese die Dauer von System-Backups etc. beschreibt)
- Wissen (ob in Büchern, Systemdokumentation oder im Kopf eines Mitarbeiters, der seit zwanzig Jahren in der Firma beschäftigt ist)

Es ist wichtig, dass Sie eine vollständige Bestandsaufnahme dieser Ressourcen durchführen, und diese *aktuell halten* — das Fehlen von "situationsbezogener Aufmerksamkeit" in Bezug auf verfügbare Ressourcen ist häufig schlimmer als *gar keine* Aufmerksamkeit.

1.5. Kennen Sie Ihre Benutzer

Auch wenn sich einige vielleicht am Begriff "Benutzer" stoßen (vielleicht durch eine abwertende Verwendung durch den Systemadministrator), ist dieser Begriff hier nicht negativ oder abwertend gemeint. Benutzer sind diejenigen, die ein System und Ressourcen, für die Sie verantwortlich sind, benutzen — nicht mehr und nicht weniger. So gesehen sind diese also Kernpunkt für Sie, um Ihre Systeme erfolgreich zu verwalten; Wenn Sie Ihre Benutzer nicht kennen und verstehen, wie können Sie dann wissen, welche Ressourcen von diesen benötigt werden?

Stellen Sie sich zum Beispiel einen Bankangestellten vor. Ein Bankangestellter verwendet einen eingeschränkten Satz an Applikationen und benötigt sehr wenig in Bezug auf Systemressourcen. Ein Software-Ingenieur auf der anderen Seite verwendet viele verschiedene Applikationen und freut sich über zusätzliche Systemressourcen (für schnellere Kompilierzeiten). Zwei komplett unterschiedliche Benutzer mit komplett unterschiedlichen Bedürfnissen.

Lernen Sie soviel über die Benutzer wie möglich.

1.6. Kennen Sie Ihren Geschäftsbereich

Ob Sie nun für ein großes, multinationales Unternehmen oder eine kleine Hochschule arbeiten, Sie müssen grundsätzlich die Art der Geschäftsumgebung, in der Sie sich befinden, verstehen. Dies läuft auf eine Frage hinaus:

Was ist der Zweck der Systeme, die Sie verwalten?

Der Schlüsselpunkt hier ist, dass Sie den Zweck Ihrer Systeme in einem globaleren Sinne verstehen.

- Applikationen, die innerhalb eines bestimmten Zeitrahmens ausgeführt werden müssen, wie zum Beispiel am Ende des Monats, Quartals oder Jahres
- Die Zeiten, in denen die Systemwartung vorgenommen wird

- Neue Technologien, die für das Lösen andauernder Probleme verwendet werden können

Indem Sie das Geschäftsfeld Ihres Unternehmens berücksichtigen, werden Sie bemerken, dass Ihre täglichen Entscheidungen besser geeignet für Ihre Benutzer und auch für Sie selber sind.

1.7. Sicherheit darf nicht vernachlässigt werden

Egal was Sie über die Umgebung denken, in der Ihre Systeme laufen, Sie können Sicherheit nicht als Selbstverständlichkeit betrachten. Auch Standalone-Systeme, die nicht mit dem Internet verbunden sind, können einem Risiko unterliegen (wenn sich dieses auch wesentlich von dem Risiko eines Systems, das mit der Außenwelt verbunden ist, unterscheidet).

Es ist sehr wichtig, dass Sie die Sicherheit von allem, was Sie tun, in Betracht ziehen. Die folgende Liste zeigt die verschiedenen Dinge, die Sie berücksichtigen sollten:

- Die Art der möglichen Bedrohungen für jedes System
- Der Ort, die Art und der Wert der Daten auf diesen Systemen
- Die Methode und Häufigkeit des berechtigten Zugriffs auf diese Systeme

Wenn Sie sich mit der Sicherheit beschäftigen, sollten Sie nicht den Fehler machen und denken, dass Eindringlinge nur von außerhalb Ihres Unternehmens einzudringen versuchen. Häufig sind Eindringlinge auch innerhalb des Unternehmens zu finden. Wenn Sie das nächste Mal durch das Büro laufen, sehen Sie sich Ihre Kollegen an und fragen Sie sich:

Was passiert, wenn *diese* Person versucht, unser Sicherheitssystem zu umgehen?

Anmerkung

Dies bedeutet *nicht*, dass Sie Ihre Kollegen als potentiell kriminell behandeln sollen. Es bedeutet nur, dass Sie sich ansehen sollten, welche Art Arbeit jeder vollbringt und inwieweit Sicherheitsverletzungen durch eine Person in dieser Position begangen werden könnten, sollte die Position ausgenutzt werden.

1.7.1. Das Risiko des Social Engineering

Während die erste Reaktion der meisten Systemadministratoren in Hinblick auf Sicherheit sich eher auf die technischen Aspekte beschränkt, sollte der gesamte Durchblick behalten werden. Häufig liegt der Ursprung von Sicherheitsverletzungen nicht in der Technik, sondern im menschlichen Wesen.

Jemand, der sich für Sicherheitsverletzungen interessiert, nutzt meistens das menschliche Wesen aus, um technische Zugangskontrollen zu umgehen. Dies wird als *Social Engineering* bezeichnet. Hier ein Beispiel:

Ein Bediener der zweiten Schicht erhält einen Telefonanruf von außerhalb der Firma. Der Anrufer gibt sich als Leiter der Finanzabteilung aus (Name und Hintergrund des Leiters wurden über die Firmenwebseite unter "Unser Team" herausgefunden).

Der Anrufer gibt vor, von einem Ort am anderen Ende der Welt anzurufen (dies kann entweder eine erfundene Geschichte sein oder vielleicht durch eine Pressemitteilung, in der das Auftreten des Finanzleiters auf einer Messe beschrieben wird, sogar Wahrheitsgehalt haben).

Der Anrufer erzählt dann eine herzzereißende Geschichte, wie sein Laptop am Flughafen gestohlen wurde und er gerade bei einem wichtigen Kunden ist und ganz dringend Zugang zum Firmenintranet benötigt, um den Kontenstand des Kunden zu prüfen. Ob der Bediener so nett wäre, die nötigen Informationen weiterzugeben?

Wissen Sie, was der Bediener in so einer Situation machten würde? Hat der Bediener keine Richtlinien (in der Form von schriftlichen Regeln und Vorgängen) denen er folgen kann, werden Sie es nicht hundertprozentig wissen.

Wie bei einer Ampel ist es das Ziel von Richtlinien, eindeutige Anleitungen für angemessenes Verhalten zu geben. Wie bei Verkehrszeichen funktionieren diese jedoch nur, wenn alle sich daran halten. Und hier liegt genau das Problem — es ist unwahrscheinlich, dass sich jeder an Ihre Richtlinien und Regeln hält. Abhängig von der Art Ihres Unternehmens ist es sogar möglich, dass Sie nicht einmal genügend Befugnis haben, Richtlinien zu definieren, geschweige denn die Einhaltung dieser zu erzwingen. Was dann?

Es gibt hierfür leider keine einfache Antwort. Benutzer-Aufklärung kann sicherlich dabei behilflich sein; Sie sollten alles tun, um der Benutzergemeinde Sicherheit und Social Engineering bewusst zu machen. Halten Sie Präsentationen über Sicherheit in der Mittagspause. Verweisen Sie auf Links zu Artikeln über Sicherheit auf Mailinglisten im Unternehmen. Stellen Sie sich als Ansprechpartner für alle Mitarbeiter zur Verfügung, sollte diesen etwas eigenartig erscheinen.

Kurz gesagt, verbreiten Sie die Nachricht an Ihre Benutzer.

1.8. Vorausplanen

Systemadministratoren, die sich all diese Ratschläge zu Herzen genommen haben und ihr Bestes getan haben, um diesen zu folgen, wären ausgezeichnete Systemadministratoren — zumindest einen Tag lang. Letzendlich wird sich die Umgebung ändern und eines Tages trifft dies unseren Systemadministrator unvorbereitet. Der Grund? Unser ansonsten so fabelhafter Systemadministrator hat nicht vorausschauend geplant.

Natürlich kann niemand die Zukunft 100% voraussagen. Mit ein bisschen Aufmerksamkeit jedoch ist es möglich, zumindest die Anzeichen von Änderungen zu erkennen.

- Eine Bemerkung am Rande während der langweiligen, wöchentlichen Mitarbeiterbesprechung über ein neues Projekt ist ein sicheres Zeichen dafür, dass Sie wahrscheinlich in naher Zukunft neue Benutzer einrichten müssen.
- Gespräche über einen anstehenden Neuerwerb bedeuten, dass Sie eventuell für neue (und vielleicht inkompatible) Systeme an einem oder mehreren Orten verantwortlich sein können.

Wenn Sie diese Zeichen erkennen (und auf diese effektiv reagieren) können, machen Sie sich und anderen das Leben leichter.

1.9. Erwarten Sie das Unerwartete

Während die Phrase "Erwarte das Unerwartete" leicht abgedroschen klingt, spiegelt dies doch die dahinterliegende Wahrheit wieder, die alle Systemadministratoren verstehen müssen:

Es *wird* Zeiten geben, in denen Sie überrascht werden.

Nachdem sich ein Systemadministrator an diese eher ungemütliche Tatsache im Leben gewöhnt hat, was kann er machen? Die Antwort liegt in Flexibilität; indem Sie Ihren Job so ausführen, dass Ihnen (und Ihren Benutzern) die meisten Optionen offen stehen. Nehmen Sie zum Beispiel Festplattenplatz. Dadurch, dass mangelnder Festplattenplatz schon fast ein Naturgesetz wie die Schwerkraft ist, ist es sinnvoll anzunehmen, dass Sie an irgendeinem Punkt mit einem dringenden Bedarf an zusätzlichem Festplattenplatz *sofort* konfrontiert werden.

Was tut ein Systemadministrator, der das Unerwartete erwartet, in diesem Fall? Vielleicht ist es möglich, ein paar Festplatten auf Lager zu haben, falls Hardwareprobleme auftreten sollten[2]. Ein Ersatz könnte dann schnell temporär eingesetzt werden[3], um den kurzfristigen Bedarf an Festplattenplatz zu decken und das Problem langfristig zu lösen (indem z.B. die Standardprozeduren für die Beschaffung zusätzlicher Festplatten befolgt werden).

Indem Sie Probleme erwarten, bevor diese auftreten, sind Sie in der Lage, schneller und effektiver zu reagieren, als wenn Sie überrascht werden.

1.10. Red Hat Enterprise Linux-spezifische Informationen

Dieser Abschnitt behandelt die Informationen, die sich auf die Philosophie der Systemadministration beziehen und speziell für Red Hat Enterprise Linux gelten.

1.10.1. Automatisierung

Die Automatisierung von häufig vorkommenden Aufgaben unter Red Hat Enterprise Linux verlangt Wissen über verschiedene Technologien. Zuallererst benötigen Sie die Befehle, die das Timing der Ausführung von Befehlen oder Skripten steuern. Die Befehle `cron` und `at` sind die dazu am häufigsten verwendeten Befehle.

Durch ein einfach zu verstehendes und dennoch leistungsstarkes zeitgesteuertes System kann `cron` die Ausführung von Befehlen oder Skripten in periodischen Abständen von Minuten bis hin zu Monaten steuern. Der Befehl `crontab` wird zur Manipulation der Dateien, die den `cron`-Daemon steuern, der wiederum jeden `cron`-Job plant, verwendet.

Der Befehl `at` (und der eng verwandte Befehl `batch`) sind besser für das Planen der Ausführung von einmaligen Skripts oder Befehlen geeignet. Diese Befehle implementieren ein rudimentäres Batch-Subsystem mit mehreren Warteschlangen und variierenden Prioritäten. Diese Prioritäten sind als *niceness* Stufen bekannt (durch den Namen des Befehls — `nice`). `at` und `batch` sind perfekt für Aufgaben, die zu einem bestimmten Zeitpunkt beginnen sollen, jedoch im Hinblick auf den Endzeitpunkt nicht zeitkritisch sind.

Als nächstes gibt es die verschiedenen Skript-Sprachen. Dies sind die "Programmiersprachen", die der durchschnittliche Systemadministrator verwendet, um den Betrieb zu automatisieren. Es gibt viele Skriptsprachen (und jeder Systemadministrator hat seine Lieblingssprache), die folgenden sind jedoch zur Zeit die am meisten gebrauchten:

- Die `bash`-Befehls-Shell
- Die `perl`-Skriptsprache
- Die `python`-Skriptsprache

Über die offensichtlichen Unterschiede dieser Sprachen hinaus ist der größte Unterschied die Art und Weise, wie diese Sprachen mit anderen Utilities auf einem Red Hat Enterprise Linux-System kommunizieren. Skripte, die mit der `bash`-Shell erstellt wurden, neigen zu einem weitläufigen Gebrauch vieler kleiner Utilities (um z.B. Zeichenketten zu manipulieren), während `perl`-Skripte diese Arten von Funktionen eher mittels Features, welche in der Sprache selbst eingebaut sind, ausführen. Ein mit `python` geschriebenes Skript kann die objektorientierten Fähigkeiten dieser Sprache voll ausnutzen und so komplexe Skripte leicht erweiterbar werden lassen.

2. Und natürlich würde ein vorausschauender Systemadministrator RAID (oder verwandte Technologien) einsetzen, um die Auswirkungen eines Ausfalls einer kritischen Festplatte zu mindern.
3. Auch hier gilt, dass vorausschauende Systemadministratoren ihre Systeme so konfigurieren, dass ein Hinzufügen einer neuen Festplatte zum System so einfach wie möglich vonstatten geht

Dies bedeutet, dass wenn Sie das Shell-Skripting wirklich beherrschen wollen, Sie sich mit den vielen Utility-Programmen (wie zum Beispiel `grep` und `sed`), die Teil von Red Hat Enterprise Linux sind, auskennen müssen. Wenn Sie `perl` (und `python`) erlernen, ist dies ein eher "eigenständiger" Prozess. Viele Konstrukte in `perl` basieren jedoch auf der Syntax verschiedener, traditioneller UNIX Utility-Programme und sind somit Red Hat Enterprise Linux-Systemadministratoren mit Erfahrung im Shell-Skripting bekannt.

1.10.2. Dokumentation und Kommunikation

Im Bereich der Dokumentation und Kommunikation gibt es wenig Spezifisches zu Red Hat Enterprise Linux. Da Dokumentation und Kommunikation aus allem Möglichen bestehen können, vom Hinzufügen von Kommentaren zu textbasierten Konfigurationsdateien bis hin zum Aktualisieren einer Webseite oder dem Versenden einer E-Mail, muss ein Red Hat Enterprise Linux-Systemadministrator Zugang zu Texteditoren, HTML-Editoren und E-Mail-Clients haben.

Hier ein kleines Beispiel der vielen unter Red Hat Enterprise Linux verfügbaren Texteditoren:

- Der Texteditor **gedit**
- Der Texteditor **Emacs**
- Der Texteditor `Vim`

Der Texteditor **gedit** ist eine rein grafische Applikation (benötigt also mit anderen Worten eine aktive X Window Systemumgebung), während `vim` und **Emacs** hauptsächlich textbasiert sind.

Die Debatte um den besten Texteditor läuft schon fast seitdem es Computer gibt und wird wohl ewig weiterlaufen. Der beste Ansatz ist wohl jeden Editor zu testen und dabei herauszufinden, welcher der Richtige für Sie ist.

Als HTML-Editoren können Systemadministratoren die Composer-Funktion im**Mozilla**-Web-Browser verwenden. Einige Systemadministratoren ziehen es vor, ihr HTML mit der Hand zu kodieren und lassen so einen herkömmlichen Texteditor zu einem vollkommen akzeptablen Tool werden.

Für E-Mail enthält Red Hat Enterprise Linux den grafischen E-Mail-Client **Evolution**, den E-Mail-Client **Mozilla** (auch grafisch) und **mutt**, welcher textbasiert ist. Wie bei den Texteditoren wird auch die Auswahl des E-Mail-Clients eher durch persönliche Vorlieben bestimmt. Der beste Ansatz ist wiederum alle zu probieren und den für Sie besten E-Mail-Client zu wählen.

1.10.3. Sicherheit

Wie bereits in diesem Kapitel erwähnt, sollte Sicherheit nicht nur ein nachträglicher Gedanke sein; Sicherheit unter Red Hat Enterprise Linux bleibt nicht nur an der Oberfläche. Authentifizierung und Zugangskontrollen sind tief in das Betriebssystem integriert und basieren auf Designs, die auf langjähriger Erfahrung der UNIX-Gemeinschaft beruhen.

Für die Authentifizierung verwendet Red Hat Enterprise Linux PAM — Pluggable Authentication Modules. PAM ermöglicht das Abstimmen der Benutzerauthentifizierung über die Konfiguration gemeinsamer Bibliotheken, die von allen PAM-kompatiblen Applikationen verwendet werden, ohne dass Änderungen an den Applikationen selbst nötig werden.

Zugangskontrolle unter Red Hat Enterprise Linux verwendet traditionelle UNIX-artige Berechtigungen (Lesen, Schreiben, Ausführen) für Benutzer, Gruppen und "Andere" Klassifikationen. Wie UNIX verwendet Red Hat Enterprise Linux auch *setuid* und *setgid*-Bits, um temporär Zugangsberechtigungen für Prozesse, die ein bestimmtes Programm ausführen, basierend auf dem Besitzer der Programmdatei zu vergeben. Dies bedeutet, dass jegliche Programme, die mit setuid- oder setgid-Berechtigungen laufen, sorgfältig auf eventuell bestehende Anfälligkeiten untersucht werden müssen.

Red Hat Enterprise Linux enthält desweiteren Support für die *Zugangskontrolllisten*. Eine Zugangskontrolllliste (ACL - Access Control List) ist ein Konstrukt, das feinabgestimmte Kontrollen über die Benutzer oder Gruppen, die auf eine Datei oder ein Verzeichnis zugreifen, ausübt. So kann z.B. eine Dateiberechtigung jeglichen Zugang zu den Dateien für alle außer dem Besitzer sperren. Die ACL der Datei kann jedoch so konfiguriert werden, dass einzig der Benutzer `bob` auf die Datei schreiben und die Gruppe `finance` die Datei lesen darf.

Ein weiterer Aspekt der Sicherheit ist die Fähigkeit, die Systemaktivitäten im Auge zu behalten. Red Hat Enterprise Linux macht ausführlichen Gebrauch von Logging auf Kernel- und auf Applikationsebene. Das Logging wird vom Systemlogging-Daemon `syslogd` gesteuert, der Systeminformationen lokal (gewöhnlich in Dateien im Verzeichnis `/var/log/`) oder auf einem Remote-System (das als Log-Server für mehrere Computer dient) aufzeichnet.

Intrusion Detection Systeme (IDS) sind leistungsstarke Tools für jeden Red Hat Enterprise Linux Systemadministrator. Ein IDS ermöglicht es Systemadministratoren festzustellen, ob unberechtigte Änderungen an einem oder mehreren Systemen vorgenommen wurden. Das allgemeine Design des Betriebssystems selbst beinhaltet IDS-ähnliche Funktionalität.

Da Red Hat Enterprise Linux mit Hilfe des RPM Paket-Managers (RPM) installiert wird, ist es möglich mit RPM festzustellen, ob Änderungen an den Paketen vorgenommen wurden, die das Betriebssystem kompromittieren könnten. Da jedoch RPM eher ein Paket-Management-Tool ist, sind dessen Fähigkeiten als IDS eingeschränkt. Es kann dennoch als erster Schritt für die Kontrolle eines Red Hat Enterprise Linux-Systems in Bezug auf unberechtigte Änderungen sein.

1.11. Zusätzliche Ressourcen

Dieser Abschnitt enthält verschiedene Ressourcen, die verwendet werden können, um mehr über die Philosophie der Systemadministration und der Red Hat Enterprise Linux-spezifischen Themen in diesem Kapitel zu lernen.

1.11.1. Installierte Dokumentation

Die folgenden Ressourcen werden mit einer typischen Installation von Red Hat Enterprise Linux mitinstalliert und können Ihnen helfen, mehr über die hier beschriebenen Themen zu erfahren.

- `crontab(1)` und `crontab(5)` man-Seiten— Lernen Sie Befehle und Scripts zur automatischen Ausführung in regelmäßigen Intervallen zu festzulegen.
- `at(1)` man-Seite — Lernen Sie Befehle und Skripte zur Ausführung zu einem späteren Zeitpunkt zu planen.
- `bash(1)` man-Seiten — Lernen Sie mehr über die Standard-Shell und das Schreiben von Shell-Skripten.
- `perl(1)` man-Seite — Links zu den vielen man-Seiten, aus denen die Online-Dokumentation von Perl besteht.
- `python(1)` man-Seite — Hier erfahren Sie mehr über die Optionen, Dateien und Umgebungsvariablen des Python-Interpreters.
- `gedit(1)` man-Seite und **Hilfe** — Lernen Sie mit diesem grafischen Texteditor das Bearbeiten von Textdateien.
- `emacs(1)` man-Seite — Lernen Sie mehr über diesen höchstflexiblen Text-Editor und dessen Online-Tutorial.
- `vim(1)` man-Seite — Lernen Sie diesen leistungsfähigen Text-Editor zu benutzen.

- **Mozilla Hilfe** — Informationen zum Bearbeiten von HTML-Dateien, Lesen von E-Mail und Browsen im Web.
- `evolution(1)` man-Seite und **Hilfe** — Informationen zum Verwalten von E-Mail mit diesem grafischen E-Mail-Client.
- `mutt(1)` man-Seite und Dateien unter `/usr/share/doc/mutt-`*<version>* — Informationen zum Verwalten von E-Mail mit diesem textbasierten E-Mail-Client.
- `pam(8)` man-Seite und Dateien unter `/usr/share/doc/pam-`*<version>* — Informationen zur Authentifizierung unter Red Hat Enterprise Linux.

1.11.2. Nützliche Webseiten

- http://www.kernel.org/pub/linux/libs/pam/ — Die Linux-PAM Projekt-Homepage.
- http://www.usenix.org/ — Die USENIX-Homepage. Eine professionelle Organisation, die sich verschrieben hat, Computerexperten aller Richtungen zusammenzubringen und verbesserte Kommunikation und Innovation zu fördern.
- http://www.sage.org/ — Die 'System Administrators Guild'-Homepage. Eine spezielle technische Gruppe in USENIX, die eine gute Ressource für alle Systemadministratoren für Linux (oder Linux-ähnliche) Betriebssysteme darstellt.
- http://www.python.org/ — Die 'Python Language'-Website. Eine hervorragende Site für weitere Informationen zu Python.
- http://www.perl.org/ — Die 'Perl Mongers'-Website. Ein guter Anfang mehr über Perl zu lernen und mit der Perl-Community in Kontakt zu treten.
- http://www.rpm.org/ — Die 'RPM Package Manager'-Homepage. Die umfangreichste Webseite zu RPM.

1.11.3. Bücher zum Thema

Die meisten Bücher zur Systemadministration behandeln die Philosophie hinter dem Job falls überhaupt nur unzureichend. Die folgenden Bücher haben jedoch Kapitel, die einige der hier angesprochenen Themen tiefergehend behandeln.

- Das *Red Hat Enterprise Linux Referenzhandbuch*; Red Hat, Inc. — Bietet einen Überblick über die Speicherorte von wichtigen Systemdateien, Benutzer- und Gruppeneinstellungen und die PAM-Konfiguration.
- Das *Red Hat Enterprise Linux Sicherheitshandbuch*; Red Hat, Inc. — Enthält eine umfangreiche Abhandlung vieler sicherheitsbezogener Fragen für Red Hat Enterprise Linux-Systemadministratoren.
- Die *Red Hat Enterprise Linux Handbuch zur System-Administration*; Red Hat, Inc. — Enthält Kapitel zur Verwaltung von Benutzern und Gruppen, Automatisieren von Aufgaben und das Verwalten von Log-Dateien.
- *Linux Administration Handbook* von Evi Nemeth, Garth Snyder und Trent R. Hein; Prentice Hall — Liefert ein gutes Kapitel über Richtlinien und die eher betriebspolitische Seite der Systemadministration einschließlich verschiedener "Was wenn"-Diskussionen über Berufsethik.
- *Linux System Administration: A User's Guide* von Marcel Gagne; Addison Wesley Professional — Enthält ein hilfreiches Kapitel zur Automatisierung verschiedener Aufgaben.
- *Solaris System Management* von John Philcox; New Riders Publishing — Wenn dieses Buch auch nicht speziell für Red Hat Enterprise Linux (oder Linux im allgemeinen) geschrieben wurde und

den Begriff "System-Manager" anstelle von "Systemadministrator" verwendet, liefert es doch einen 70-seitigen Überblick über die Rolle, die Systemadministratoren in einem typischen Unternehmen spielen.

Kapitel 2.

Ressourcenkontrolle

Wie bereits erwähnt dreht sich ein Großteil der Systemadminsitration um Ressourcen und deren effizienten Einsatz. Indem verschiedene Ressourcen und die Mitarbeiter und Programme, die diese verwenden, miteinander abgeglichen werden, verschwenden Sie einerseits weniger Geld und haben andererseits mit glücklicheren Mitarbeitern zu tun. Dies lässt jedoch zwei Fragen offen:

Was sind Ressourcen?

und:

Wie stelle ich fest, welche Ressourcen verwendet werden (und in welchem Ausmaß)?

Der Zweck dieses Kapitels ist es, diese Fragen zu beantworten und Ihnen dabei zu helfen, mehr über Ressourcen und deren Überwachung zu erfahren.

2.1. Grundlegende Konzepte

Bevor Sie Ressourcen überwachen können, müssen Sie zuallererst wissen, welche Ressourcen es zu überwachen gibt. Alle Systeme besitzen folgende Ressourcen:

- Prozessorleistung
- Bandbreite
- Speicher
- Speicherplatz

Diese Ressourcen werden tiefergehend in den folgenden Abschnitten beschrieben. Zur Zeit müssen Sie jedoch nur im Hinterkopf behalten, dass diese Ressourcen einen direkten Einfluss auf die Systemleitung und daher auf die Produktivität Ihrer Benutzer haben.

Im Grunde ist das Überwachen von Ressourcen nichts weiter als das Sammeln von Informationen über die Verwendung einer oder mehrere Systemressourcen.

Dies ist jedoch meistens nicht ganz so einfach. Als Erstes müssen Sie die Ressourcen, die überwacht werden sollen, in Betracht ziehen. Danach ist es notwendig, jedes System zu überprüfen, das überwacht werden soll, insbesondere in Hinblick auf deren Situation.

Die zu überwachenden Systeme fallen in zwei Kategorien:

- Das System erfährt zur Zeit Leistungseinbußen und Sie möchten die Leistung verbessern.
- Das System läuft einwandfrei und Sie möchten, dass dies so bleibt.

Die erste Kategorie bedeutet, dass Sie die Ressourcen vom Blickpunkt der Systemleistung überwachen, während die zweite Kategorie bedeutet, dass Sie die Ressourcen eher in Hinblick auf die Kapazitätsplanung überwachen sollten.

Da jede Perspektive ihre eigenen Anforderungen hat, beschreiben die folgenden Abschnitte jede der Kategorien im Detail.

2.2. System-Leistungskontrolle

Wie bereits erwähnt wird das Überwachen der Systemleistung meistens als Reaktion auf Leistungsprobleme durchgeführt. Entweder ist das System zu langsam oder Programme werden gar nicht ausgeführt (und manchmal fällt das gesamte System aus). In jedem Fall wird die Überwachung der Systemleistung als erster und letzter Schritt in einem Drei-Schritte-Vorgang ausgeführt:

1. Überwachung, um die Art und Umfang der Ressourceneinbrüche, die den Leistungsgabfall verursachen, zu identifizieren
2. Die hieraus hervorgehenden Daten werden ausgewertet und Maßnahmen zur Problemlösung (meistens Leistungstuning und/oder die Beschaffung zusätzlicher Hardware) eingeleitet
3. Überwachung, um sicher zu gehen, dass das Problem gelöst wurde

Aus diesem Grund ist die Systemleistungskontrolle eher von kurzer Dauer und detaillierter im Umfang.

Anmerkung

Die Systemleistungskontrolle ist häufig ein wiederholungsreicher Prozess, da diese Schritte mehrmals wiederholt werden müssen, um die bestmögliche Systemleistung zu erreichen. Der Hauptgrund hierfür ist, dass die Systemressourcen und deren Einsatz eng miteinander verbunden sind, sodass z.B. durch das Beseitigen eines Engpasses häufig auch ein anderer entdeckt wird.

2.3. Überwachen der Systemkapazität

Das Überwachen der Systemkapazität ist Teil eines fortlaufenden Programms zur Kapazitätsplanung. Die Kapazitätsplanung verwendet Langzeitüberwachung von Ressourcen, um Änderungen im Einsatz von Systemressourcen festzustellen. Sobald diese Änderungen bekannt sind, ist es möglich, genauere Langzeit-Pläne für die Beschaffung zusätzlicher Ressourcen zu erstellen.

Die Überwachung zum Zwecke der Kapazitätsplanung unterscheidet sich von der Leistungsüberwachung auf zwei Arten:

- Die Überwachung findet mehr-oder-weniger kontinuierlich statt
- Die Überwachung ist üblicherweise nicht so detailliert

Der Grund für diese Unterschiede liegt in der Zielsetzung eines Kapazitätplanungs-Programms. Kapazitäsplanung erfordert den Blickpunkt des "Big Picture"; kurzfristige oder anomale Ressourcenverwendung ist von geringem Interesse. Daten werden über einen gewissen Zeitraum gesammelt, was die Einteilung der Ressourcenverwendung in Bezug auf Änderungen der Last ermöglicht. In engerdefinierten Umgebungen (in denen z.B. nur eine Applikation ausgeführt wird) ist es möglich, den Einfluss der Applikation auf die Systemressourcen darzustellen. Dies kann mit genügend Exaktheit erreicht werden, wodurch Sie z.B. feststellen können, welchen Auswirkungen fünf weitere Mitarbeiter haben, die auf die Applikation am geschäftigsten Zeitpunkt des Tages zugreifen.

2.4. Was überwachen?

Wie bereits erwähnt sind die Ressourcen in jedem System CPU-Leistung, Bandbreite, Speicher und Speicherplatz. Auf den ersten Blick scheint es, dass die Überwachung sich nur um die Untersuchung dieser vier Dinge dreht.

Leider ist es nicht ganz so einfach. Denken Sie zum Beispiel an eine Festplatte. Was würden Sie gerne über deren Leistungsfähigkeit erfahren?

- Wieviel freier Platz steht zur Verfügung?
- Wieviele I/O-Operationen werden pro Sekunde durchschnittlich ausgeführt?
- Wie lange dauert es, bis jede I/O-Operation abgeschlossen ist?
- Wieviele dieser I/O-Operationen sind Lesen? Wieviele Schreiben?
- Was ist die durchschnittliche Größe von Daten, die mit jedem I/O gelesen/geschrieben werden?

Es gibt natürlich weitere Methoden zur Untersuchung der Festplattenleistung. Die oben genannten Punkte haben sich nur mit einem winzigen Teil des Ganzen beschäftigt. Das Hauptkonzept ist, dass es viele verschiedene Datentypen für jede Ressource gibt.

Die folgenden Abschnitte beschäftigen sich mit den Arten der Nutzungsinformationen, die für jede der Hauptressourcen hilfreich sind.

2.4.1. Überwachung der CPU-Leistung

In seiner einfachsten Form bedeutet die Überwachung der CPU-Leistung nicht mehr als festzustellen, ob die CPU-Ausnutzung 100% erreicht. Liegt diese Ausnutzung unter 100%, egal was das System gerade macht, steht weitere Prozess-Leistung zur Verfügung.

Es ist jedoch selten, dass Systeme die 100% CPU-Ausnutzung nicht zumindest manchmal erreichen. An diesem Punkt ist es wichtig, die CPU-Ausnutzungsdaten eingehender zu betrachten. Hierdurch können Sie dann feststellen, wo der Hauptteil der Prozess-Leistung genutzt wird. Hier finden Sie einige der bekannteren CPU-Nutzungsstatistiken:

Benutzer versus System

> Der Prozentsatz der Zeit, der auf Benutzer-basierte Verarbeitung im Gegensatz zu System-basierter Verarbeitung aufgewendet wird, kann aufzeigen, ob die Systemlast durch ausgeführte Applikationen oder durch eine Überlastung des Betriebssystems verursacht wird. Hohe Benutzer-basierte Prozentsätze sind ein gutes Zeichen (solange die Benutzer mit der Leistung zufrieden sind), während hohe System-basierte Prozentsätze Probleme aufzeigen, die eventuell weitere Nachforschung erfordern.

Context-Switches

> Ein Context-Switch findet dann statt, wenn die CPU einen Prozess beendet und damit beginnt einen neuen Prozess auszuführen. Da jeder Context-Switch vom Betriebssystem verlangt, Kontrolle über die CPU zu erhalten, gehen exzessive Context-Switches und hoher CPU-Verbrauch auf System-Ebene Hand in Hand.

Interrupts

> Wie der Name besagt (Interrupts; engl. für Unterbrechungen) sind Interrupts Situationen, bei denen die Verarbeitung der CPU abrupt unterbrochen wird. Interrupts treten häufig aufgrund von Hardware-Aktivitäten (z.B. ein I/O-Gerät schließt eine I/O-Operation ab) oder aufgrund von Software (z.B. Software-Interrupts, die die Verarbeitung von Applikationen steuern) auf. Da Interrupts auf System-Ebene behoben werden müssen, führen hohe Interrupt-Raten zu erhöhtem CPU-Verbrauch auf System-Ebene.

Ausführbare Prozesse

> Ein Prozess kann sich in verschiedenen Zuständen befinden. So zum Beispiel:
>
> - Wartend, dass eine I/O abgeschlossen wird

- Wartend auf das Speicher-Verwaltungs-Subsystem, dass ein Seitenfehler behoben wird

In diesen Umständen hat der Prozess keinen Bedarf für die CPU.

Irgendwann ändert sich jedoch der Prozess-Status und der Prozess wird ausgeführt. Ein ausführbarer Prozess führt, wie der Name schon sagt, Aufgaben aus, sobald dieser dazu Zeit von der CPU erhält. Werden jedoch mehr als ein Prozess [1] ausgeführt, so müssen alle Prozesse bis auf einen Prozess warten, bis diese an der Reihe sind. Indem Sie die Anzahl der ausführbaren Prozesse überwachen, können Sie feststellen, wie stark Ihr System eingebunden ist.

Andere Leistungs-Metriken, welche die Auswirkung auf die CPU-Ausnutzung veranschaulichen, umfassen verschiedene Services, die das Betriebssystem den Prozessen bereitstellt. Dies können Statistiken zur Speicherverwaltung, I/O-Verarbeitung und so weiter sein. Diese Statistiken zeigen außerdem, dass wenn die Leistung überwacht wird, es keine Grenzen zwischen den verschiedenen Statistiken gibt. Mit anderen Worten heißt dies, dass die CPU-Ausnutzungsstatistiken ein Problem im I/O-Subsystem anzeigen oder dass die Speichernutzungsstatistik einen Designfehler in einer Applikation aufzeigen kann.

Wenn Sie daher die Systemleistung überwachen, ist es nicht möglich, nur eine Statistik isoliert zu betrachten. Lediglich indem Sie das gesamte Bild betrachten, können Sie wichtige Informationen aus den Leistungsstatistiken herausziehen.

2.4.2. Überwachung der Bandbreite

Das Überwachen der Bandbreite ist schwieriger als die anderen hier beschriebenen Ressourcen. Der Grund hierfür ist, dass Leistungsstatistiken eher auf Geräten basieren, während die Bandbreite eher in Bezug auf Busse, die die Geräte verbinden, wichtig ist. In solchen Fällen, in denen ein Gerät einen allgemeinen Bus teilt, sehen Sie zwar normale Statistiken für jedes Gerät, die gesammelte Last auf den Geräten am Bus ist jedoch wesentlich größer.

Eine weitere Herausforderung bei der Überwachung der Bandbreite ist der Umstand, dass es vorkommen kann, dass Statistiken für die Geräte nicht verfügbar sind. Dies gilt insbesondere für System-Erweiterungsbusse und Datenpfade[2]. Auch wenn 100% exakte Bandbreiten-Statistiken nicht immer zur Verfügung stehen, gibt es jedoch meistens genügend Informationen, um einen gewissen Analyse-Grad zu erreichen; insbesondere dann, wenn verwandte Statistiken berücksichtigt werden.

Einige der häufigeren Bandbreiten-bezogenen Statistiken sind:

Bytes empfangen/gesendet

Netzwerk-Schnittstellen-Statistiken liefern einen Anhaltspunkt für die Bandbreitennutzung auf einem der offensichtlicheren Busse — dem Netzwerk.

Schnittstellen-Counts und -Raten

Diese Netzwerk-bezogenen Statistiken geben Hinweise auf übermäßige Kollisionen, übertragene und empfangene Fehler und vieles mehr. Durch diese Statistiken (insbesondere wenn diese für mehr als ein System im Netzwerk zur Verfügung stehen) ist es möglich, Problembehebung im Netzwerk durchzuführen, bevor allgemeinere Netzwerk-Diagnose-Tools eingesetzt werden müssen.

Übertragungen pro Sekunde

Normalerweise für I/O-Block-Geräte wie Festplatten und Hochleistungs-Bandgeräte ist diese Statistik eine gute Methode festzustellen, ob die Bandbreite für ein bestimmtes Gerät ausgelastet ist. Durch ihre elektro-mechanische Natur können Festplatten und Bandgeräte nur eine gewissen

1. auf einem Einzel-Prozessor Computersystem
2. Weitere Informationen zu Bussen, Datenpfaden und Bandbreite finden Sie unter Kapitel 3

Anzahl von I/O-Operationen pro Sekunde ausführen. Deren Leistung sinkt erheblich, wenn diese Grenze erreicht wird.

2.4.3. Überwachung von Speicher

Es gibt nur einen Bereich, in dem eine Vielzahl an Leistungsstatistiken gefunden werden können. Dies ist die Überwachung der Speichernutzung. Durch die inhärente Komplexität moderner Betriebssysteme mit virtuellem Speicher auf Bedarfsbasis sind Statistiken zur Speichernutzung zahlreich und höchst unterschiedlich. In diesem Bereich findet ein Großteil der Arbeit eines Systemadministrators für das Ressourcenmanagement statt.

Die folgenden Statistiken stellen einen groben Überblick über allgemeine Speicher-Management-Statistiken dar:

Page-Ins/Page-Outs

Durch diese Statistiken kann der Fluss von Seiten vom Systemspeicher zu Massenspeichergeräten (Festplatten) gemessen werden. Hohe Raten dieser Statistiken bedeuten, dass das System zu wenig physikalischen Speicher hat und *überlastet* ist oder mehr Systemressourcen auf das Verschieben von Seiten in und aus dem Speicher aufwendet, als auf das eigentliche Ausführen von Applikationen.

Aktive/Inaktive Seiten

Diese Statistik zeigt, wie stark speicherresidente Seiten verwendet werden. Ein Fehlen inaktiver Seiten kann auf ein Fehlen von ausreichendem physikalischem Speicher hinweisen.

Freie, gemeinsam benutzte, gepufferte und gecachete Seiten

Diese Statistiken liefern zusätzlich Details zu den einfacheren 'Aktive/Inaktive Page'-Statistiken. Durch das Verwenden dieser Statistik ist es möglich, die gesamte Verwendung des Speichers festzustellen.

Swap-Ins/Swap-Outs

Diese Statistiken zeigen das Swapping-Verhalten des gesamten Systems. Übermäßige Raten können hier auf Unzulänglichkeiten im physikalischen Speicher hinweisen.

Die erfolgreiche Überwachung der Speichernutzung erfordert ein grundlegendes Verständnis über die Funktionsweise von Betriebssystemen mit virtuellem Speicher auf Bedarfsbasis. Während dieses Thema allein ein ganzes Buch umfassen kann, werden die Grundkonzepte unter Kapitel 4 beschrieben. Dieses Kapitel, zusammen mit der Zeit, die Sie mit der Überwachung des Systems verbringen, gibt Ihnen den Grundstein für das aufzubauende Verständnis dieses Themas.

2.4.4. Überwachen von Speicherplatz

Das Überwachen des Speicherplatzes findet auf zwei verschiedenen Ebenen statt:

- Auf ausreichenden Festplattenplatz hin überwachen
- Auf Speicher-bezogene Leistungsprobleme hin überwachen

Der Grund hierfür ist die Möglichkeit schwerwiegende Probleme in dem einen Bereich zu haben und gar keine Probleme in einem anderen Bereich. Es ist zum Beispiel möglich, dass eine Festplatte nicht mehr über genügend Speicher verfügt, ohne dass dieser Umstand auch nur ein einziges mal leistungsbezogene Probleme aufwirft. Andererseits ist es möglich, dass eine Festplatte 99% freien Platz hat, jedoch in Bezug auf das Leistungsverhalten deren eigene Grenzen überschreitet.

Es ist jedoch wahrscheinlicher, dass das durchschnittliche System variierende Grade von Ressourcen-Einbußen in beiden Kategorien erfährt. Es ist daher auch wahrscheinlich, dass — zu einem gewissen Grad — Probleme in einem Bereich zu Problemen im anderen Bereich führen. Der häufigste Typ dieser Interaktion nimmt die Form geringer und geringer werdender I/O-Leistung an, wenn eine Festplatte fast keinen freien Platz mehr besitzt.

In jeden Fall sind die folgenden Statistiken nützlich für das Überwachen von Speicherplatz:

Freier Platz

Freier Platz ist wahrscheinlich die Ressource, die von allen Systemadministratoren genauestens überwacht wird. Es ist ziemlich selten, dass ein Systemadministrator niemals den freien Platz überprüft (oder einen automatisierten Weg dafür gefunden hat).

Dateisystem-bezogene Statistiken

Diese Statistiken (wie z.B. über die Anzahl von Dateien/Verzeichnissen, die durchnittliche Dateigröße etc.) liefern zusätzliche Details über den Prozentsatz freien Festplattenplatzes. Diese Statistiken ermöglichen es Adminisratoren, das System für die bestmögliche Leistung zu konfigurieren, da die I/O-Last von einem Dateisystem mit einer Vielzahl kleiner Dateien sich von der eines Systems mit einer einzigen, riesigen Datei unterscheidet.

Übertragungen pro Sekunde

Diese Statistik ist eine gute Methode festzustellen, ob die Grenzen der Bandbreite auf einem bestimmten Gerät erreicht wurden.

Lese-/Schreibvorgänge pro Sekunde

Als eine ein wenig detailliertere Analyse von Übertragungen pro Sekunde, ermöglichen diese Statistiken dem Systemadministrator die Natur der I/O-Lasten, die ein Speichergerät erfährt, besser zu verstehen. Dies kann kritisch sein, da einige Technologien sehr unterschiedliche Performance-Merkmale für Lese- versus Schreib-Operationen aufweisen.

2.5. Red Hat Enterprise Linux-spezifische Informationen

Red Hat Enterprise Linux wird mit einer Reihe von Ressourcenüberwachungstools ausgeliefert. Während es mehr Tools als die hier aufgeführten gibt, sind diese hier charakteristisch für Funktionalität. Die Tools sind:

- `free`
- `top` (und **GNOME System Monitor**, eine grafisch orientierte Versionen von `top`)
- `vmstat`
- Die Sysstat-Suite an Ressourcenkontrolletools
- Der systemweite OProfile-Profiler

Lassen Sie uns jedes dieser Tools im Detail betrachten.

2.5.1. `free`

Der `free`-Befehl zeigt die Speicherausnutzung an. Hier ein Beispiel der Ausgabe:

```
             total       used       free     shared    buffers     cached
Mem:        255508     240268      15240          0       7592      86188
-/+ buffers/cache:     146488     109020
```

```
Swap:       530136      26268     503868
```

Die Zeile `Mem:` zeigt die Nutzung des physikalischen Speichers, während `Swap:` die Ausnutzung des System-Swap-Platzes zeigt. Die Zeile `-/+ buffers/cache:` zeigt die Größe des physikalischen Speichers an, welcher derzeit den Systempuffern gehört.

Da `free` standardmäßig die Informationen zur Speichernutzung nur einmal anzeigt, ist er nur nützlich für kurzzeitiges Überwachen oder zum raschen Feststellen, ob ein Speicher-bezogenes Problem vorliegt. Auch wenn `free` die Fähigkeit hat, wiederholt die Daten zur Speichernutzung über die Option `-s` anzuzeigen, läuft die Ausgabe relativ schnell über den Bildschirm, was ein Auffinden von Änderungen in der Speichernutzung schwierig gestaltet.

Tipp

Eine bessere Lösung als `free -s` ist das Ausführen von `free` mit dem `watch`-Befehl. Um zum Beispiel die Speichernutzung alle zwei Sekunden anzuzeigen (das Standard-Intervall für `watch`), verwenden Sie den folgenden Befehl:

```
watch free
```

Der `watch`-Befehl gibt den Befehl `free` alle zwei Sekunden aus und löscht vorher den Bildschirm. Dies macht es wesentlich einfacher festzustellen, wie sich die Speichernutzung über eine gewisse Zeit hinweg ändert, da Sie nicht ständig über den Bildschirm laufenden Output durchsuchen müssen. Sie können die Verzögerung zwischen den Aktualisierungen mit der Option `-n` kontrollieren und können alle Änderungen zwischen Updates markieren lassen, indem Sie die Option `-d` wie im folgenden Befehl verwenden:

```
watch -n 1 -d free
```

Weitere Informationen finden Sie auf der `watch` man-Seite.

Der `watch`-Befehl wird solange ausgeführt, bis dieser mit [Strg]-[C] unterbrochen wird. Der `watch`-Befehl kann in vielen Situationen nützlich sein und sollte daher im Gedächtnis behalten werden.

2.5.2. `top`

Während `free` nur Speicher-bezogene Informationen anzeigt, bietet der `top`-Befehl ein wenig von Allem. CPU-Nutzung, Prozess-Statistiken, Speichernutzung — `top` überwacht all dies. Zusätzlich dazu und im Gegensatz zu `free` ist das Standardverhalten von `top` kontinuierlich abzulaufen. Der `watch`-Befehl wird nicht benötigt. Dazu ein Beispiel:

```
 14:06:32  up 4 days, 21:20,  4 users,  load average: 0.00, 0.00, 0.00
77 processes: 76 sleeping, 1 running, 0 zombie, 0 stopped
CPU states:  cpu    user    nice  system    irq  softirq  iowait    idle
           total   19.6%    0.0%    0.0%   0.0%     0.0%    0.0%  180.2%
           cpu00    0.0%    0.0%    0.0%   0.0%     0.0%    0.0%  100.0%
           cpu01   19.6%    0.0%    0.0%   0.0%     0.0%    0.0%   80.3%
Mem:  1028548k av,  716604k used,  311944k free,       0k shrd,  131056k buff
                    324996k actv,  108692k in_d,   13988k in_c
Swap: 1020116k av,    5276k used, 1014840k free                  382228k cached

  PID USER     PRI  NI  SIZE  RSS SHARE STAT %CPU %MEM   TIME CPU COMMAND
17578 root      15   0 13456  13M  9020 S    18.5  1.3  26:35   1 rhn-applet-gu
19154 root      20   0  1176 1176   892 R     0.9  0.1   0:00   1 top
    1 root      15   0   168  160   108 S     0.0  0.0   0:09   0 init
    2 root      RT   0     0    0     0 SW    0.0  0.0   0:00   0 migration/0
    3 root      RT   0     0    0     0 SW    0.0  0.0   0:00   1 migration/1
```

```
  4 root      15   0     0     0     0 SW    0.0  0.0   0:00   0 keventd
  5 root      34  19     0     0     0 SWN   0.0  0.0   0:00   0 ksoftirqd/0
  6 root      35  19     0     0     0 SWN   0.0  0.0   0:00   1 ksoftirqd/1
  9 root      15   0     0     0     0 SW    0.0  0.0   0:07   1 bdflush
  7 root      15   0     0     0     0 SW    0.0  0.0   1:19   0 kswapd
  8 root      15   0     0     0     0 SW    0.0  0.0   0:14   1 kscand
 10 root      15   0     0     0     0 SW    0.0  0.0   0:03   1 kupdated
 11 root      25   0     0     0     0 SW    0.0  0.0   0:00   0 mdrecoveryd
```

Die Anzeige ist in zwei Abschnitte unterteilt. Der obere Abschnitt enthält Informationen zum Gesamtstatus des Systems — Laufzeit, Lastdurchschnitt, Prozesszahlen, CPU-Status und Nutzungsstatistiken für Speicher und Swap-Space. Im unteren Abschnitt werden Statistiken auf Prozess-Ebene angezeigt, die gesteuert werden können, wenn `top` ausgeführt wird. Zum Beispiel zeigt `top` lediglich Prozesse an, auch wenn ein Prozess multi-threaded ist. Um die einzelnen Threads anzuzeigen, drücken Sie [i]. Um zur Standardanzeige zurückzukehren, drücken Sie diese Taste nocheinmal.

Achtung

Auch wenn `top` wie ein einfaches, reines Anzeige-Programm erscheint, ist dies nicht der Fall. Dies liegt daran, dass `top` sog. Einzelzeichen-Befehle für die verschiedenen Aufgaben verwendet. Wenn Sie zum Beispiel als root angemeldet sind, können Sie die Priorität eines Prozesses ändern oder diesen stoppen. Solange Sie nicht die Hilfe zu `top` gelesen haben (drücken Sie [?] für die Anzeige) ist es am sichersten, nur [q] einzugeben (wodurch Sie `top` verlassen).

2.5.2.1. Der GNOME System Monitor — Ein grafischer `top`-Befehl

Wenn Sie grafische Oberflächen vorziehen, ist vielleicht der **GNOME System Monitor** eher für Sie geeignet. Wie `top` zeigt der **GNOME System Monitor** Informationen in Bezug auf den Gesatmstatus des Systems, Prozesszahlen, Speicher- und Swap-Nutzung sowie Statistiken auf Prozessebene an.

Der **GNOME System Monitor** geht noch einen Schritt weiter, indem er eine grafische Darstellung von CPU, Speicher und Swap-Nutzung sowie eine tabellenförmige Nutzungsliste zum Festplattenplatz anzeigt. Ein Beispiel der **GNOME System Monitor Prozessliste** finden Sie unter Abbildung 2-1.

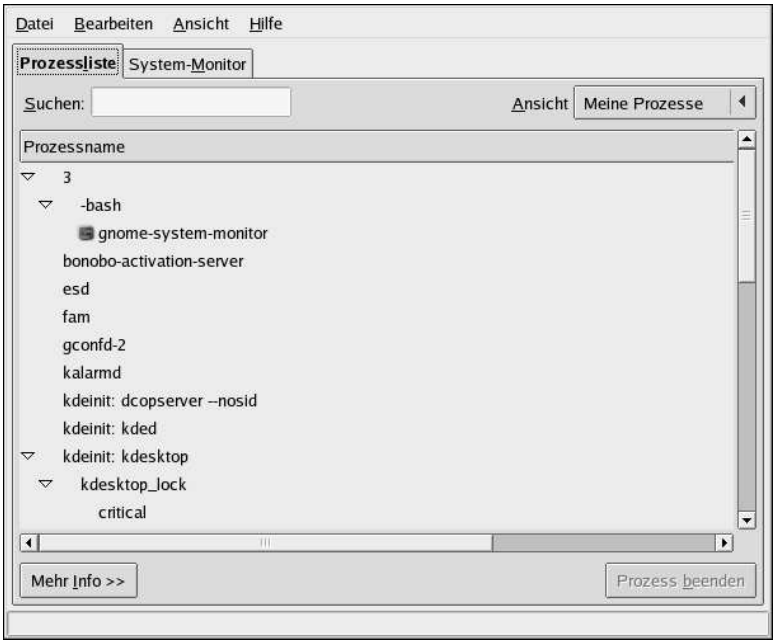

Abbildung 2-1. Anzeige der GNOME System Monitor Prozessliste

Zusätzliche Informationen können für einen bestimmten Prozess angezeigt werden, indem Sie den gewünschten Prozess auswählen und dann auf **Mehr Info** klicken.

Um Statistiken zu CPU, Speicher und Festplattennutzung anzuzeigen, klicken Sie auf **System Monitor**.

2.5.3. `vmstat`

Für ein präziseres Verständnis der Systemleistung versuchen Sie es doch einfach mit `vmstat`. Mit `vmstat` erhalten Sie einen Überblick über Prozesse, Speicher, Swap, I/O, System und CPU-Aktivität in einer einzigen Zahlenreihe:

```
procs                  memory      swap          io     system         cpu
 r  b   swpd   free   buff  cache   si   so    bi    bo   in    cs us sy id wa
 0  0   5276 315000 130744 380184    1    1     2    24   14    50  1  1 47  0
```

Die erste Zeile unterteilt das Feld in sechs Kategorien, inklusive Prozesse, Speicher, Swap, I/O, System und CPU Statistiken. Die zweite Zeile identifiziert den Inhalt jeden Feldes, was das rasche und einfache Suchen nach bestimmten Statistiken innerhalb der Daten ermöglicht.

Die Prozess-bezogenen Felder sind:

- `r` — Die Anzahl ausführbarer Prozesse, die auf Zugriff zur CPU warten
- `b` — Die Anzahl der Prozesse in einem nicht-unterbrechbaren Sleep-State (Throttel-State)

Die Speicher-bezogenen Felder sind:

- `swpd` — Die Größe des verwendeten virtuellen Speichers
- `free` — Freier Speicher
- `buff` — Größe des für Puffer verwendeten Speichers
- `cache` — Speicher, der als Page-Cache verwendet wird

Die Swap-bezogenen Felder sind:

- `si` — Der Speicher, der von der Festplatte geswappt wurde
- `so` — Der Speicher, der auf die Festplatte geswappt wurde

Die I/O-bezogenen Felder sind:

- `bi` — An ein Blockgerät gesendete Blöcke
- `bo` — Von einem Blockgerät empfangene Blöcke

Die system-bezogenen Felder sind:

- `in` — Die Anzahl der Interrupts pro Sekunde
- `cs` — Die Anzahl der Context-Switches pro Sekunde

Die CPU-bezogenen Felder sind:

- `us` — der Prozentsatz der Zeit, in der die CPU Benutzer-Level Code ausführt
- `sy` — der Prozentsatz der Zeit, in der die CPU System-Level Code ausführt
- `id` — der Prozentsatz der Zeit, in der die CPU im Leerlauf war
- `wa` — Eingang/Ausgang warten

Wird `vmstat` ohne Optionen ausgeführt, wird nur eine Zeile angezeigt. Diese Zeile enthält Durchschnitte, die von der Zeit an berechnet wurden, zu der das System das letzte Mal gebootet wurde.

Die meisten Administratoren verlassen sich jedoch nicht auf die Daten in dieser Zeile, da die Zeit, in der diese gesammelt werden, variiert. Stattdessen nutzen sie den Vorteil von `vmstats` Fähigkeit, Ressourcendaten zu bestimmten Intervallen wiederholt anzuzeigen. So zeigt zum Beispiel der Befehl `vmstat 1` eine neue Ressourcenzeile jede Sekunde an, während der Befehl `vmstat 1 10` eine neue Zeile pro Sekunde anzeigt; jedoch nur für die nächsten zehn Sekunden.

In den Händen eines erfahrenen Administrators kann `vmstat` zum idealen Werkzeug werden, um rasch Ressourcen-Nutzung und Leistungsprobleme feststellen zu können. Für einen tieferen Einblick wird eine andere Art von Tool benötigt — ein Tool, das eine tiefgreifendere Datenerfassung und -analyse ermöglicht.

2.5.4. Die Sysstat-Suite von Ressourcenüberwachungstools

Während die oben genannten Tools dabei hilfreich sein können, mehr Einblick in die Leistungsfähigkeit eines Systems über sehr kurze Zeiträume hinweg zu bekommen, sind diese nicht von großem Nutzen, wenn mehr als nur ein Schnappschuß der Systemressourcenauslastung benötigt wird. Zusätzlich gibt es einige Aspekte der Leistungsfähigkeit eines Systems, die nicht einfach mittels solcher simplistischen Tools überwacht werden können.

Deshalb ist ein anspruchsvolleres Tool notwendig. Sysstat ist ein solches Tool.

Sysstat beinhaltet die folgenden Tools in Bezug auf das Sammeln von Eingabe/Ausgabe- und CPU-Statistiken:

`iostat`

Gibt einen Überblick über die CPU-Auslastung, gemeinsam mit I/O-Statistiken für eines oder für mehrere Laufwerke.

`mpstat`

Zeigt detaillgenauere CPU-Statistiken an.

Sysstat beinhaltet ebenso Tools, die Daten zur Systemressourcenauslastung sammeln und tägliche, auf diesen Daten basierende Reporte erstellen. Diese Tools sind:

`sadc`

Bekannt als System Activity Data Collector, sammelt der Befehl `sadc` Systemressourcen-Informationen und schreibt diese in eine Datei.

`sar`

`sar`-Reporte, die aus den von `sadc` erstellten Dateien erzeugt werden, können entweder interaktiv generiert werden oder für eine intensivere Analyse in eine Datei geschrieben werden.

Die folgenden Abschnitte erforschen jedes einzelne dieser Tools in allen Einzelheiten.

2.5.4.1. Der `iostat`-Befehl

Der `iostat`-Befehl vermittelt grundsätzlich einen Überblick über CPU- und Eingang/Ausgang-Statistiken:

```
Linux 2.4.20-1.1931.2.231.2.10.ent (pigdog.example.com)      07/11/2003

avg-cpu:  %user   %nice    %sys   %idle
           6.11    2.56    2.15   89.18

Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
dev3-0            1.68        15.69        22.42   31175836   44543290
```

Unter der ersten Zeile (welche die Kernelversion des Systems und den Hostnamen gemeinsam mit dem aktuellen Datum beinhaltet), zeigt `iostat` einen Überblick über die durchschnittliche CPU-Auslastung des Systems seit dem letzten Reboot-Vorgang an. Der CPU-Auslastungs-Report beinhaltet folgende Prozentsätze:

- Prozentualer Anteil der Zeit, die im Benutzermodus verbracht wurde (laufende Applikationen, usw.)
- Prozentualer Anteil der Zeit, die im Benutzermodus verbracht wurde (für Prozesse, deren Planungsprioritäten mittels `nice(2)` geändert wurden)
- Prozentualer Anteil der Zeit, die im Kernelmodus verbracht wurde
- Prozentualer Anteil der Zeit, die im Leerlauf verbracht wurde

Unter dem Report zur CPU-Auslastung ist der Geräte-Auslastungs-Report anzufinden. Dieser Report beinhaltet eine Zeile für jedes einzelne aktive Platten-Device auf dem System und beinhaltet die folgenden Informationen:

- Die Gerätespezifikation, dargestellt als dev<*major-number*>-*sequence-number*, wobei <*major-number*> die Major-Nummer des Gerätes darstellt[3] und <*sequence-number*> eine aufeinanderfolgende Nummer ist, welche mit Null beginnt.
- Die Transferhäufigkeit (oder Eingabe/Ausgabe-Operationen) pro Sekunde.
- Die Anzahl von 512-Byte-Blöcken, die pro Sekunde gelesen wurden.
- Die Anzahl von 512-Byte-Blöcken, die pro Sekunde beschrieben wurden.
- Die Gesamtanzahl von 512-Byte-Blöcken, die gelesen wurden.
- Die Gesamtanzahl von 512-Byte-Blöcken, die beschrieben wurden.

Dies ist nur ein Beispiel der Information, welche mittels dem `iostat`-Befehl erlangt werden können. Für weitere Informationen siehe die `iostat(1)` man-Seite.

2.5.4.2. Der `mpstat`-Befehl

Der `mpstat`-Befehl erscheint zunächst keine Unterschiede zum CPU-Auslastungs-Report aufzuweisen, welcher mittels dem `iostat`-Befehl erstellt wurde:

```
Linux 2.4.20-1.1931.2.231.2.10.ent (pigdog.example.com)      07/11/2003

07:09:26 PM  CPU   %user   %nice %system   %idle    intr/s
07:09:26 PM  all    6.40    5.84    3.29   84.47    542.47
```

Mit der Ausnahme einer zusätzlichen Spalte, welche die CPU-bezogenen Interrupts pro Sekunde anzeigt, gibt es keinen wirklichen Unterschied. Jedoch ändert sich dies, wenn die `mpstats -P ALL`-Option verwendet wird:

```
Linux 2.4.20-1.1931.2.231.2.10.ent (pigdog.example.com)      07/11/2003

07:13:03 PM  CPU   %user   %nice %system   %idle    intr/s
07:13:03 PM  all    6.40    5.84    3.29   84.47    542.47
07:13:03 PM    0    6.36    5.80    3.29   84.54    542.47
07:13:03 PM    1    6.43    5.87    3.29   84.40    542.47
```

Auf Multiprozessor-Systemen ermöglicht `mpstat` die Auslastung für jede CPU individuell anzuzeigen, um feststellen zu können, wie effektiv jede CPU genutzt wird.

2.5.4.3. Der `sadc`-Befehl

Wie bereits zuvor beschrieben, werden durch den `sadc`-Befehl Systemauslastungsdaten gesammelt, die zur Analyse zu einem späteren Zeitpunkt in eine Datei geschrieben werden. Standardmäßig werden die Daten in Dateien geschrieben, die sich im Verzeichnis `/var/log/sa/` befinden. Die Dateien werden `sa`<*dd*> genannt, wobei <*dd*> das aktuelle zweistellige Datum ist.

`sadc` wird normalerweise vom `sa1`-Script durchgeführt. Dieses Script wird periodisch durch `cron` über die Datei `sysstat` aufgerufen, welche sich in `/etc/cron.d/` befindet. Das `sa1`-Script ruft `sadc` zu einem einzelnen einsekündigen Messintervall auf. Standardmäßig bringt`cron sa1` alle 10 Minuten zum ablaufen, wobei die gesammelten Daten während jedem Intervall zur aktuellen `/var/log/sa/sa`<*dd*>-Datei hinzugefügt werden.

3. Major-Nummern von Geräten können mittels `ls -l`gefunden werden, um die gewünschte Geräte-Datei in `/dev/` anzuzeigen. Die Major-Nummer erscheint nach der Gruppenspezifikation des Gerätes.

2.5.4.4. Der `sar`-Befehl

Der `sar`-Befehl erzeugt System-Nutzungs-Reporte basierend auf Daten, die von `sadc` gesammelt wurden. Die Red Hat Enterprise Linux-Konfigurierung lässt `sar` automatisch ablaufen, um die Dateien zu verarbeiten, welche ebenso automatisch von `sadc` gesammelt werden. Die Report-Dateien werden in `/var/log/sa/` geschrieben und `sar`<*dd*> genannt, wobei <*dd*> das Datum des vorhergehenden Tages zweistellig darstellt.

`sar` wird normalerweise mittels `sa2`-Script durchgeführt. Dieses Script wird periodisch durch `cron` über die Datei `sysstat` aufgerufen, welche sich in `/etc/cron.d/` befindet. Standardmäßig lässt `cron` den Befehl `sa2` einmalt täglich um 23:53 ablaufen, wobei ein Report über die sämtlichen Daten des jeweiligen Tages erstellt wird.

2.5.4.4.1. Das Lesen von `sar`-Reporten

Das Format eines `sar`-Reportes, der durch die standardmäßige Konfiguration von Red Hat Enterprise Linux erstellt worden ist, besteht aus verschiedenen Sektionen, wobei jede Sektion eine spezifische Art von Daten enthält; gegliedert nach dem Zeitpunkt, zu dem diese gesammelt wurden. Da `sadc` dahingehend konfiguriert ist, alle zehn Minuten einen ein-sekündigen Messintervall auszuführen, beinhalten die standardmäßigen `sar`-Reporte Daten in zehn-minütigen Abschnitten von 00:00 bis 23:50 Uhr[4].

Jeder Abschnitt des Reports beginnt mit einem Titel, welcher die in diesem Abschnitt enthaltenen Daten beschreibt. Der Titel wird in regelmäßigen Abständen im gesamten Abschnitt wiederholt. Dies vereinfacht die Auswertung der Daten, während man durch den Report blättert. Jeder Abschnitt endet mit einer Zeile, die den Durchschnitt der im jeweiligen Abschnitt behandelten Daten angibt.

Hier ist ein Beispielabschnitt zu einem `sar`-Report ohne den Daten von 00:30 bis 23:40 Uhr, um Platz zu sparen:

```
00:00:01          CPU     %user     %nice   %system     %idle
00:10:00          all      6.39      1.96      0.66     90.98
00:20:01          all      1.61      3.16      1.09     94.14
...
23:50:01          all     44.07      0.02      0.77     55.14
Average:          all      5.80      4.99      2.87     86.34
```

In diesem Abschnitt wird die CPU-Auslastungsinformation angezeigt. Diese sind den durch `iostat` angezeigten Daten sehr ähnlich.

Andere Abschnitte können auch mehr als eine Daten-Zeile zu einem bestimmten Zeitpunkt aufweisen, wie in diesem Abschnitt über CPU-Nutzungsdaten ersichtlich ist, welche auf einem Dual-Prozessorsystem gesammelt wurden:

```
00:00:01          CPU     %user     %nice   %system     %idle
00:10:00            0      4.19      1.75      0.70     93.37
00:10:00            1      8.59      2.18      0.63     88.60
00:20:01            0      1.87      3.21      1.14     93.78
00:20:01            1      1.35      3.12      1.04     94.49
...
23:50:01            0     42.84      0.03      0.80     56.33
23:50:01            1     45.29      0.01      0.74     53.95
Average:            0      6.00      5.01      2.74     86.25
Average:            1      5.61      4.97      2.99     86.43
```

4. Infolge sich ständig ändernder Systemlasten kann der genaue Zeitpunkt, an dem die Daten gesammelt wurden, um ein bis zwei Sekunden variieren.

Es gibt eine Gesamtanzahl von siebzehn verschiedenen Abschnitten in Reporten, die mittels der standardmäßigen Red Hat Enterprise Linux `sar`-Konfiguration erstellt werden. Einige werden in den folgenden Kapiteln näher behandelt. Für nähere Informationen über die Daten in den einzelnen Abschnitten siehe die `sar(1)` man-Seite.

2.5.5. OProfile

Der systemweite Profiler OProfile ist ein Low-Overhead Überwachungstool. OProfile benutzt dazu die Leistungskontrolle-Hardware des Prozessors[5], um die Natur leistungsbezogener Probleme genau festzustellen.

Leistungskontrolle-Hardware ist ein Teil des Prozessors selbst. In Form eines speziellen Counters, dessen Wert sich jedes mal erhöht, wenn ein bestimmter Vorgang (z.B. wenn der Prozessor sich nicht im Leerlauf befindet (nicht idle ist) oder die angeforderten Daten nicht im Cache aufzufinden sind) stattfindet. Einige Prozessoren besitzen mehr als einen solchen Counter und erlauben dadurch die Selektion unterschiedlicher Arten von Vorgängen für jeden einzelnen Counter.

Die Counter können mit einem anfänglichen Wert geladen werden und erzeugen jedes mal ein Interrupt im Falle eines Counter-Overflows. Durch das Laden eines Counters mit verschiedenen anfänglichen Werten, ist es möglich die Rate zu variieren, zu der Interrupts erzeugt werden. Auf diese Art ist es möglich, die Sample-Rate zu kontrollieren und somit auch den Grad an Detailgenauigkeit in Hinsicht auf die gesammelten Daten zu bestimmen.

In einem Extremfall würde die Einstellung des Counters, sodass dieser einen Overflow-Interrupt bei jedem Vorgang erzeugt, den Erhalt extrem detaillierter Leistungsdaten (jedoch mit massivem Overhead) bedeuten. Im entgegengesetzten Extremfall würde die Einstellung des Counters, sodass dieser so wenige Interrupts als möglich erzeugt, lediglich den Erhalt eines höchst allgemeinen System-Überblicks bedeuten (mit praktisch keinem Overhead). Das Geheimnis einer effektiven Überwachung ist die Auswahl einer Sample-Rate, welche ausreichend hoch ist, um die erforderlichen Daten zu erfassen, wobei das System jedoch gleichzeitig nicht mit Leistungskontrolle-Overhead überlastet wird.

Achtung

Sie können OProfile derart konfigurieren, sodass es ausreichend Overhead produziert, um das System unbenutzbar zu machen. Deshalb müssen Sie Vorsicht walten lassen, wenn Sie Counter-Werte auswählen. Aus diesem Grund unterstützt der `opcontrol`-Befehl die `--list-events`-Option, welche die vorhandenen Event-Typen für den gegenwärtig installierten Prozessor gemeinsam mit den jeweils empfohlenen Minimal-Counter-Werten anzeigt.

Es ist wichtig einen Kompromiss zwischen Sample-Rate und Overhead einzugehen, wenn Sie OProfile benutzen.

2.5.5.1. OProfile-Komponenten

OProfile besteht aus folgenden Komponenten:

- Datenerfassungssoftware
- Datenanalysesoftware
- Administrative Schnittstellen-Software

5. OProfile kann ebenso einen Fallback-Mechanismus (als TIMER_INT bekannt) benutzen, falls in Systemarchitekturen Performance-Monitoring-Hardware nicht vorhanden ist.

Die Datenerfassungssoftware besteht aus dem `oprofile.o` Kernel-Modul und dem `oprofiled`-Daemon.

Die Datenanalysesoftware beinhaltet folgende Programme:

`op_time`

Zeigt die Anzahl und den relativen Prozentsatz von Samples (Proben) für jede einzelne ausführbare Datei an.

`oprofpp`

Zeigt die Anzahl und den relativen Prozentsatz von Samples an, die entweder durch eine Funktion, individuelle Befehle oder in Form einer `gprof`-stil Ausgabe erstellt worden sind

`op_to_source`

Zeigt kommentierten Sourcecode und/oder Assemblerprotokolle an

`op_visualise`

Zeigt gesammelte Daten graphisch an

Diese Programme machen es möglich, gesammelte Daten in einer Vielzahl von Arten anzuzeigen.

Die administrative Schnittstellen-Software kontrolliert alle Aspekte der Datensammlung, von der genauen Bestimmung, welche Art von Daten kontrolliert werden müssen bis hin zum Start- und Anhaltevorgang des eigentlichen Sammelvorganges. Dies kann mittels `opcontrol`-Befehl durchgeführt werden.

2.5.5.2. Beispiel für eine OProfile-Sitzung

Dieser Abschnitt zeigt eine OProfile Kontroll- und Datenanalyse-Sitzung von der ursprünglichen Konfiguration bis hin zur schlussendlichen Datenanalyse. Dies ist lediglich ein einleitender Überblick. Für detailliertere Informationen, verweisen wir auf das *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Benutzen Sie `opcontrol`, um den Datentyp zu konfigurieren, welcher mittels folgendem Befehl gesammelt werden soll:

```
opcontrol \
    --vmlinux=/boot/vmlinux-‘uname -r‘ \
    --ctr0-event=CPU_CLK_UNHALTED \
    --ctr0-count=6000
```

Die hierbei benutzten Optionen dienen zur Ausrichtung von `opcontrol`:

- Richten Sie OProfile auf eine Kopie des derzeit laufenden Kernels aus (`--vmlinux=/boot/vmlinux-‘uname -r‘`)
- Legen Sie fest, dass der Prozessor-Counter 0 benutzt wird und dass das Event, welches kontrolliert werden soll, der Zeitpunkt ist, an dem von der CPU Instruktionen ausgeführt werden (`--ctr0-event=CPU_CLK_UNHALTED`)
- Legen Sie fest, dass OProfile jedes 6000ste mal Samples nimmt, wenn das spezifizierte Event erfolgt (`--ctr0-count=6000`)

Als nächstes überprüfen Sie, dass das `oprofile`-Kernelmodul mittels dem Befehl `lsmod` geladen ist:

```
Module                  Size  Used by    Not tainted
oprofile               75616   1
...
```

Gehen Sie sicher, dass das OProfile Dateisystem (befindlich in `/dev/oprofile/`) mit dem Befehl `ls /dev/oprofile/` gemountet wird:

```
0  buffer       buffer_watershed  cpu_type  enable       stats
1  buffer_size  cpu_buffer_size   dump      kernel_only
```

(Die genaue Anzahl von Dateien variiert mit dem Prozessortyp.)

An dieser Stelle beinhaltet die `/root/.oprofile/daemonrc`-Datei die Einstellungen, die für die Datenerfassungs-Software erforderlich sind:

```
CTR_EVENT[0]=CPU_CLK_UNHALTED
CTR_COUNT[0]=6000
CTR_KERNEL[0]=1
CTR_USER[0]=1
CTR_UM[0]=0
CTR_EVENT_VAL[0]=121
CTR_EVENT[1]=
CTR_COUNT[1]=
CTR_KERNEL[1]=1
CTR_USER[1]=1
CTR_UM[1]=0
CTR_EVENT_VAL[1]=
one_enabled=1
SEPARATE_LIB_SAMPLES=0
SEPARATE_KERNEL_SAMPLES=0
VMLINUX=/boot/vmlinux-2.4.21-1.1931.2.349.2.2.entsmp
```

Als nächstes benutzen Sie `opcontrol`, um die Datenerfassung mittels `opcontrol --start`-Befehl zu starten:

```
Using log file /var/lib/oprofile/oprofiled.log
Daemon started.
Profiler running.
```

Gehen Sie sicher, dass der `oprofiled`-Daemon mittels dem Befehl `ps x | grep -i oprofiled` läuft:

```
32019 ?        S      0:00 /usr/bin/oprofiled --separate-lib-samples=0 ...
32021 pts/0    S      0:00 grep -i oprofiled
```

(Die eigentliche durch `ps` angezeigte `oprofiled`-Befehlszeile ist viel länger, wurde hier jedoch zu Formatierzwecken abgeschnitten.)

Das System wird nunmehr kontrolliert, wobei die Daten für alle auf dem System befindlichen, ausführbaren Events gesammelt werden. Die Daten werden in dem `/var/lib/oprofile/samples/`-Verzeichnis gespeichert. Die Dateien in diesem Verzeichnis unterliegen einer eher ungewöhnlichen Namenskonvention. Hier ist ein Beispiel:

```
}usr}bin}less#0
```

Die Namenskonvention benutzt den absoluten Pfad jeder einzelnen Datei, die ausführbaren Code enthält, wobei die Schrägstriche (`/`) durch rechte geschweifte Klammern (`}`) ersetzt werden und mit einem Rautenzeichen (`#`) enden, gefolgt von einer Nummer (in diesem Fall `0`.) Deshalb verkörpert die in diesem Beispiel verwendete Datei diejenigen Daten, welche während `/usr/bin/less` gesammelt worden sind.

Sobald Daten gesammelt worden sind, benutzen Sie eines der Analysetools, um diese anzuzeigen. Ein gutes Leistungsmerkmal von OProfile ist der Umstand, dass es nicht notwendig ist die Datenerfassung zu stoppen, bevor man eine Datenanalyse durchführt. Jedoch müssen Sie zuwarten, bis zumindest ein

Satz von Samples auf die Platte geschrieben wird oder Sie zwingen diese Samples mittels `opcontrol --dump` auf die Platte.

Im folgendem Beispiel wird der Befehl `op_time` dazu benutzt, um die erfassten Daten (in umgekehrter Reihenfolge —beginnend mit der höchsten Anzahl von Samples, danach absteigend) anzuzeigen:

```
3321080   48.8021  0.0000 /boot/vmlinux-2.4.21-1.1931.2.349.2.2.entsmp
761776    11.1940  0.0000 /usr/bin/oprofiled
368933     5.4213  0.0000 /lib/tls/libc-2.3.2.so
293570     4.3139  0.0000 /usr/lib/libgobject-2.0.so.0.200.2
205231     3.0158  0.0000 /usr/lib/libgdk-x11-2.0.so.0.200.2
167575     2.4625  0.0000 /usr/lib/libglib-2.0.so.0.200.2
123095     1.8088  0.0000 /lib/libcrypto.so.0.9.7a
105677     1.5529  0.0000 /usr/X11R6/bin/XFree86
...
```

Es ist sicherlich eine gute Idee `less` zu benutzen, wenn ein Report interaktiv erzeugt wird, da dieser Hunderte von Zeilen lang sein kann. Das hier gezeigte Beispiel ist aus diesem Grund abgeschnitten worden.

Das Format für diesen speziellen Report setzt sich aus jeweils einer Zeile für jede einzelne ausführbare Datei zusammen, für die Samples erzeugt wurden. Jede Zeile entspricht dem selben Format:

<sample-count> *<sample-percent>* *<unused-field>* *<executable-name>*

Wo:

- *<sample-count>* steht für die Anzahl von erfassten Abfragen.
- *<sample-percent>* steht für den Prozentsatz aller Abfragen, welche für diese spezifische, ausführbare Datei gesammelt worden sind
- *<unused-field>* steht für ein unbenutztes Feld
- *<executable-name>* steht für den Namen der Datei, die ausführbaren Code besitzt und wofür Anfragen getätigt worden sind.

Dieser Report (auf einem zumeist im Leerlauf befindlichen System) zeigt, dass beinahe die Hälfte aller Samples genommen wurden, während die CPU Kernel-Code ausführt. Als nächstes finden Sie den OProfile Datenerfassungs-Daemon, gefolgt von einer Vielzahl von Dokumentationen und dem X Window System Server, `XFree86`. Bitte beachten Sie, dass für das hierbei verwendete System ein Counter-Wert von 6000 verwendet wurde, was gleichzeitig der von `opcontrol --list-events` empfohlene Minimumwert ist. Dies bedeutet, dass — zumindest für dieses spezielle System — OProfile-Overhead zu keinem Zeitpunkt mehr als rund 11% der CPU-Leistung verbraucht.

2.6. Zusätzliche Ressourcen

Dieser Abschnitt beinhaltet verschiedene Ressourcen, die dazu benutzt werden können, um mehr über Ressourcenkontrolle und dem Red Hat Enterprise Linux-spezifischen Thema herauszufinden, welches in diesem Kapitel behandelt wurde.

2.6.1. Installierte Dokumentation

Die folgenden Ressourcen werden im Laufe einer typischen Red Hat Enterprise Linux-Installation mitinstalliert.

- `free(1)` man-Seite — Lernen Sie Statistiken bezüglich freiem und genutztem Speicher anzuzeigen.
- `top(1)` man-Seite — Lernen Sie CPU-Auslastungs- und Prozessebenen-Statistiken anzuzeigen.
- `watch(1)` man-Seite — Lernen Sie das vorgegebene Programm in periodischen Abständen auszuführen und dabei Vollbildschirmausgabe zu verwenden.
- **GNOME System Monitor Hilfe**-Menü Eintrag — Lernen Sie Prozess-, CPU-, Speicher- und Speicherplatzauslastungs-Statistiken grafisch darzustellen.
- `vmstat(8)` man-Seite —Lernen Sie eine kurze Zusammenfassung der Prozess-, Speicher-, Swap-, I/O-, System- und CPU-Auslastung darzustellen.
- `iostat(1)` man-Seite — Lernen Sie CPU- und I/O-Statistiken anzuzeigen.
- `mpstat(1)` man-Seite — Lernen Sie individuelle CPU-Statistiken auf Multiprozessor-Systemen anzuzeigen.
- `sadc(8)` man-Seite — Lernen Sie Systemauslastungsdaten zu sammeln.
- `sa1(8)` man-Seite — Lernen Sie mehr über ein Script, das `sadc` periodisch ablaufen lässt.
- `sar(1)` man-Seite — Lernen Sie Nutzungsberichte über System-Ressourcen zu erstellen.
- `sa2(8)` man-Seite — Lernen Sie tägliche Nutzungsberichte-Dateien in Bezug auf System-Ressourcen zu erstellen.
- `nice(1)` man-Seite — Lernen Sie die Prozessplanungsprioritäten zu ändern.
- `oprofile(1)` man-Seite — Lernen Sie ein Profil der Systemfunktionen zu erstellen.
- `op_visualise(1)` man-Seite — Lernen Sie OProfile-Daten grafisch darzustellen.

2.6.2. Nützliche Webseiten

- http://people.redhat.com/alikins/system_tuning.html — System-Tuning-Informationen für Linux-Server. Eine 'Bewusstseinsstrom' geprägteBetrachtungsweise zum Thema Performance-Tuning und Ressourcenüberwachung für Server.
- http://www.linuxjournal.com/article.php?sid=2396 — Tools zur Performance-Kontrolle für Linux. Diese Linux Journalseite ist mehr in Richtung Administrator ausgelegt, der darin interessiert ist, eine maßgeschneiderte Lösung zur Darstellung eines Leistungsdiagrammes zu schreiben. Bereits vor einigen Jahren geschrieben, kann es sein, dass einige Details nicht mehr länger zutreffend sind; Gesamtkonzept und Ausführung sind jedoch einwandfrei.
- http://oprofile.sourceforge.net/ — OProfile Projekt-Webseite. Beinhaltet nützliche OProfile Ressourcen, inklusive Pointers zu Mailinglisten und dem #oprofile IRC Channel.

2.6.3. Themenbezogene Literatur

Die folgenden Bücher behandeln verschiedenste Themen in Bezug auf Ressourcenkontrolle und sind gute Nachschlagewerke für Red Hat Enterprise Linux-Systemadministratoren:

- *Red Hat Enterprise Linux Handbuch zur System-Administration*; Red Hat, Inc. — Beinhaltet Information über viele der Überwachungstools, die hier behandelt wurden, wie z.B. auch OProfile.
- *Linux Performance Tuning and Capacity Planning* von Jason R. Fink und Matthew D. Sherer; Sams — Gibt einen mehr ins Detail gehenden Überblick über die hier vorgestellten Tools zur Ressourcenkontrolle und beinhaltet auch andere Tools, die sich bestens für spezifischere Ressourcenkontrollbedürfnisse eignen.

- *Red Hat Linux Security and Optimization* von Mohammed J. Kabir; Red Hat Press — Ungefähr die ersten 150 Seiten dieses Buches behandeln leistungsbezogene Themen. Dies beinhaltet Kapitel, die Leistungsfragen in Bezug auf Netzwerk, Internet, E-Mail und Dateiservern behandeln.
- *Linux Administration Handbook* von Evi Nemeth, Garth Snyder und Trent R. Hein; Prentice Hall — Stellt ein kurzes Kapitel zur Verfügung, welches sich in einem ähnlichen Rahmen wie dieses Buch befindet; mit Ausnahme eines interessanten Abschnittes über die Diagnose eines Systems, das plötzlich langsamer geworden ist.
- *Linux System Administration: A User's Guide* von Marcel Gagne; Addison Wesley Professional — Beinhaltet ein kurzers Kapitel über Leistungskontrolle und Tuning.

Kapitel 3.

Bandbreite und Prozessleistung

Von den zwei Ressourcen, die in diesem Kapitel beschrieben werden, ist eine davon (Bandbreite) oft für den Systemadministrator nicht einfach zu verstehen, während die andere (Prozessleistung) zumeist einem einfach zu verstehenderen Konzept unterliegt.

Zusätzlich dazu mag der Anschein erweckt werden, dass diese beiden Ressourcen nicht eng miteinander verbunden sind — warum also gemeinsam behandeln?

Der Grund dafür, dass beide Ressourcen gemeinsam behandelt werden, ist derjenige, dass diese Ressourcen auf Hardware basieren, welche in direktem Zusammenhang mit der Fähigkeit eines Computers Daten zu transportieren und zu verarbeiten stehen.

3.1. Bandbreite

Grundsätzlich ist Bandbreite die Kapazität zur Datenübertragung — in anderen Worten, wieviele Daten in einem bestimmten Zeitraum von einem Punkt zum anderen transportiert werden können. Eine Punkt-zu-Punkt Datenkommunikation setzt folgende zwei Dinge voraus:

- Einen Satz elektrische Leiter, um eine Kommunikation auf unterster Ebene möglich zu machen
- Ein Protokoll, um die effiziente und verlässliche Kommunikation von Daten zu erleichtern

Es gibt zwei Arten von Systemkomponenten, die diesen Anforderungen entsprechen:

- Busse
- Datenpfade

Die folgenden Abschnitte untersuchen diese in allen Einzelheiten.

3.1.1. Busse

Wie zuvor angegeben, ermöglichen Busse Punkt-zu-Punkt Kommunikation und benutzewn eine Art Protokoll, um sicher zu gehen, dass jegliche Kommunikation auf eine kontrollierte Art abläuft. Jedoch haben Busse auch andere charakteristische Merkmale:

- Standardisierte, elektrische Merkmale (wie zum Beispiel die Anzahl von Leitern, Spannungspegel, Übertragungsgeschwindigkeit, usw.)
- Standardisierte, mechanische Merkmale (wie die Art von Stecker, Kartengröße, physikalische Anordnung, usw.)
- Standardisiertes Protokoll

Das Wort "standardisiert" ist wichtig, da Busse die hauptsächliche Form darstellen, in der verschiedene Systemkomponenten verbunden werden.

In vielen Fällen erlauben Busse die Verbindung von Hardware unterschiedlicher Hersteller; ohne Standardisierung wäre dies nicht möglich. Jedoch auch in Situationen, in denen ein Bus urheberrechtliches Eigentum eines bestimmten Erzeugers ist, ist Standardisierung ein wichtiger Punkt, der dem Erzeuger erlaubt auf einfachere Weise verschiedene Komponenten zu implementieren, wobei eine allgemeine Schnittstelle verwendet wird — nämlich der Bus selbst.

3.1.1.1. Beispiele von Bussen

Ganz egal wo Sie bei einem Computersystem nachschauen, finden Sie Busse. Hier sind einige der gebräuchlicheren Busse:

- Massenspeicher-Busse (ATA und SCSI)
- Netzwerke[1] (Ethernet und Token Ring)
- Speicher-Busse (PC133 und Rambus®)
- Expansions-Busse (PCI, ISA, USB)

3.1.2. Datenpfade

Datenpfade können schwerer zu identifizieren sein, sind jedoch wie Busse überall anzutreffen. Genauso wie Busse ermöglichen auch Datenpfade Punkt-zu-Punkt-Kommunikation. Jedoch im Gegensatz zu Bussen:

- Benutzen Datenpfade ein einfacheres Protokoll (falls überhaupt)
- Besitzen Datenpfade wenig (falls überhaupt) mechanische Standardisierung

Der Grund dafür ist, dass Datenpfade normalerweise systemintern sind und nicht dazu benutzt werden, ad-hoc die Verknüpfung zwischen verschiedenen Komponenten herzustellen. Als solches sind Datenpfade höchst optimiert auf bestimmte Situationen, in denen Geschwindigkeit und geringe Kosten gegenüber langsamerer und teurerer Mehrzweck-Flexibilität vorgezogen werden.

3.1.2.1. Beispiele von Datenpfaden

Hier sind einige typische Datenpfade:

- 'CPU zu On-Chip Cache'-Datenpfad
- 'Grafik Prozessor zu Video-Speicher'-Datenpfad

3.1.3. Potentielle Bandbreiten-bezogene Probleme

Es gibt zwei Arten auf denen Probleme, die auf Bandbreiten bezogen sind, entstehen können (entweder für Busse oder Datenpfade):

1. Der Bus oder Datenpfad kann eine gemeinsam benutzte Ressource darstellen. In diesem Fall wird durch die dadurch für den Bus entstehende Konkurrenzsituation die effektive Bandbreite reduziert, die für alle Geräte am Bus erhältlich ist.

   Ein SCSI-Bus mit einigen höchst aktiven Laufwerken wäre ein gutes Beispiel dafür. Die höchst aktiven Laufwerke sättigen den SCSI-Bus, wobei nur wenig Bandbreite für jegliche andere Geräte auf dem selben Bus übrig bleibt. Als Endergebnis sind alle I/O-Vorgänge in Verbindung mit irgendeinem der Geräte auf diesem Bus langsam, sogar wenn jedes einzelne Geräte auf dem Bus nicht übermäßig aktiv ist.
2. Der Bus oder Datenpfad kann eine fest zugeordnete Ressource mit einer festgelegten Anzahl von angeschlossenen Geräten sein. In diesem Fall schränken die elektrischen Eigenschaften des Busses (und in gewisser Weise auch die Art des benutzten Protokolls) die erhältliche Bandbreite

1. Anstatt eines Intra-System-Bus, können Netzwerke auch als *Inter*-System-Bus angesehen werden.

ein. Dies ist normalerweise häufiger bei Datenpfaden als bei Bussen der Fall. Dies ist auch einer der Gründe, warum Grafik-Adapter dazu neigen, bei höheren Auflösungen oder Farbtiefen langsamer zu arbeiten — Bei jedem Auffrischen des Bildschirms müssen mehr Daten entlang des Datenpfads transportiert werden, welcher Videospeicher und Grafikprozessor miteinander verbindet.

3.1.4. Potenzielle, Bandbreiten-bezogene Lösungen

Glücklicherweise kann auf Probleme, die sich auf Bandbreite beziehen, reagiert werden. Tatsächlich gibt es einige unterschiedliche Vorgehensweisen:

- Die Last verteilen
- Die Last reduzieren
- Die Kapazität erhöhen

Die folgenden Abschnitte befassen sich genauer mit jeder Vorgehensweise:

3.1.4.1. Verteilen der Last

Die erste Annäherung ist die gleichmäßigere Verteilung der Bus-Aktivität. In anderen Worten, wenn ein Bus überlastet und ein anderer frei ist, so könnte die Situation wahrscheinlich dadurch verbessert werden, dass einiges der Arbeitslast an den freien Bus weitergeleitet wird.

Als Systemadministrator ist dies die erste Methode, die sie in Betracht ziehen sollten, da des öfteren bereits zusätzliche Busse in ihrem System vorhanden sind. Zum Beispiel beinhalten die meisten PCs mindestens zwei ATA-*Channels* (was nur eine andere Bezeichnung für Bus ist). Wenn Sie zwei ATA-Laufwerke besitzen und zwei ATA-Channels, warum sollten dann beide Laufwerke auf dem selben Channel sein?

Auch wenn Ihre Systemkonfiguration keine zusätzlichen Busse beinhaltet, so kann auch die reine Verteilung der Last eine vernünftige Lösung darstellen. Die Ausgaben für Hardware, um dies zu bewerkstelligen, wären immer noch geringer, als wenn ein bestehender Bus durch Hardware mit höherer Kapazität ausgetauscht werden müsste.

3.1.4.2. Reduzieren der Last

Auf den ersten Blick scheinen das Verteilen und das Reduzieren der Last lediglich verschiedene Seiten der selben Münze zu sein. Immerhin gilt, dass wenn man die Last verteilt, dies gleichzeitig die Last reduziert (zumindest auf dem überlasteten Bus), richtig?

Während dieser Standpunkt zwar korrekt erscheint, hat das Verteilen der Last jedoch nicht die selbe Auswirkung, als das *globale* Reduzieren der Last. Der Schlüssel dazu liegt in der Ermittlung, ob ein gewisser Aspekt in der Systemlast zur Überlastung des jeweiligen Busses führt. Kann es sein, dass zum Beispiel ein Netzwerk schwerstens überlastet ist aufgrund unnötiger Aktivitäten? Vielleicht ist auch eine kleine temporäre Datei der Empfänger enormer Lese-/Schreib-Eingänge/Ausgänge? Wenn sich diese temporäre Datei auf einem im Netzwerk befindlichen Dateiserver befindet, so könnte viel Netzwerkverkehr vermieden werden, wenn z.B. lokal mit dieser Datei gearbeitet wird.

3.1.4.3. Die Kapazität erhöhen

Die offensichtliche Lösung für ungenügende Bandbreite ist diese irgendwie zu erhöhen. Jedoch ist dies normalerweise ein teures Unterfangen. Nehmen wir zum Beispiel einen SCSI-Controller und dessen überlasteten Bus. Um dessen Bandbreite zu erhöhen, müsste der SCSI-Controller (und wahrscheinlich alle angehängten Geräte) gegen schnellere Hardware ausgetauscht werden. Wenn der SCSI-Controller eine separate Karte ist, dann wäre dies ein relativ unkomplizierter Prozess. Wenn der SCSI-

Controller jedoch ein Teil der Hauptplatine ist, so wird es zusehends schwerer den ökonomischen Punkt einer solchen Veränderung zu rechtfertigen.

3.1.5. Im Überblick...

Alle Systemadministratoren sollten sich über Bandbreite und die Auswirkungen von System-Konfiguration und -Benutzung auf die Bandbreite im Klaren sein. Leider ist es nicht immer offensichtlich, wenn es sich bei einem Problem um ein Bandbreiten-Problem handelt. Manchmal ist der Bus selbst nicht das Problem, dafür eine der Komponenten, welche mit dem Bus verbunden sind.

Stellen Sie sich zum Beispiel einen SCSI-Adapter vor, der mit einem PCI-Bus verbunden ist. Im Falle von Performance-Problemen mit dem SCSI-Festplatten-I/O kann dies das Ergebnis eines dürftig ausführenden SCSI-Adapters sein, auch wenn die SCSI- und PCI-Busse nicht im Geringsten deren eigentliche Bandbreiten-Fähigkeiten erreicht haben.

3.2. Prozessleistung

Oft auch als CPU-Leistung, CPU-Zyklen und unter zahlreichen anderen Namen bekannt, ist Prozessleistung die Fähigkeit eines Computers Daten zu manipulieren. Prozessleistung variiert mit der Architektur (und der Taktrate) der CPU — normalerweise besitzen CPUs mit höherer Taktrate und diejenigen, die größere Datentypen unterstützen, eine höhere Prozessleistung als langsamere CPUs, welche kleinere Datentypen unterstützen.

3.2.1. Fakten über Prozessleistung

Hier sind die zwei Hauptfakten über Prozessleistung, die Sie im Gedächtnis behalten sollten:

- Prozessleistung ist fix
- Prozessleistung kann nicht gespeichert werden

Die Prozessleistung ist ein fixer Wert, daher kann die CPU nur eine bestimmte Geschwindigkeit erreichen. Wenn Sie zum Beispiel zwei Nummern zusammenzählen müssen (ein Vorgang, bei dem nur eine Maschinen-Instruktion in den meisten Architekturen benötigt wird), so kann eine spezielle CPU dies lediglich mit einer Geschwindigkeit tun. Mit wenigen Ausnahmen ist es nicht einmal möglich die CPU-Rate bei der Bearbeitung von Befehlen zu *verlangsamen*; die Chancen diese zu erhöhen sind noch geringer.

Prozessleistung ist auch auf eine andere Art fix festgelegt: Sie ist begrenzt/endlich. Die Arten von CPUs, die an irgendeinen Computer angeschlossen werden können, sind begrenzt. Einige Systeme unterstützen eine Vielzahl von verschiedenen CPUs von unterschiedlicher Geschwindigkeit, während andere Systeme dahingehend überhaupt nicht upgradbar sind[2].

Prozessleistung kann nicht für einen späteren Gebrauch gespeichert werden. In anderen Worten bedeutet dies, dass wenn eine CPU 100 Millionen Befehle in einer Sekunde verarbeiten kann, in einer Sekunde Leerlauf gleichzeitig 100 Millionen verarbeitungswürdige Befehle verschwendet worden sind.

Wenn wir diese Tatsachen von einer etwas unterschiedlicheren Perspektive aus betrachten, so "produziert" eine CPU einen Strom von ausgeführten Befehlen zu einem bestimmten Satz. Und wenn eine CPU ausgeführte Befehle "produziert", so bedeutet dies gleichzeitig, dass etwas anderes diese "konsumiert". Der nächste Abschnitt definiert diese sogenannten Konsumenten.

2. Diese Situation führt zu einem humorvoll genannten *'Forklift Upgrade' (Gabelstapler Upgrade)*, was soviel wie das Ersetzen des gesamten Computers bedeutet.

3.2.2. Konsumenten der Prozessleistung

Es gibt zwei Hauptkonsumenten von Prozessleistung:

- Applikationen
- Das Betriebssystem selbst

3.2.2.1. Applikationen

Die offensichtlichsten Konsumenten von Prozessleistung sind die Applikationen und Programme, welche Sie vom Computer ausgeführt haben möchten. Von der Kalkulationstabelle bis zur Datenbank, Applikationen sind der Grund dafür, dass Sie überhaupt einen Computer besitzen.

Ein Einzel-CPU-System kann immer nur eine Sache auf einmal tun. Deshalb gilt, dass wenn Ihre Applikation gerade läuft, alles andere auf Ihrem System nicht ablaufen kann. Und natürlich umgekehrt — wenn etwas anderes als Ihre Applikation abläuft, dann steht dafür Ihre Applikation still.

Aber wie kommt es, dass viele verschiedene Applikationen dem Anschein nach auf einem modernen Betriebssystem gleichzeitig ablaufen? Die Antwort darauf ist, dass es sich dabei um Multitasking-Betriebssysteme (Betriebssysteme mit Mehrprogrammbetrieb) handelt. In anderen Worten erzeugen diese die Illusion, dass mehrere Dinge gleichzeitig geschehen, obwohl dies in Wirklichkeit nicht möglich ist. Der Trick dabei ist, jedem Prozess einen Bruchteil einer Sekunde Laufzeit auf der CPU zu geben, bevor die CPU an einen anderen Prozess für wiederum einen Bruchteil einer Sekunde weitergegeben wird. Wenn diese *'Context-Switches' (Änderungen des Inhaltes)* häufig genug stattfinden, so wird die Illusion von mehreren gleichzeitig laufenden Applikationen vermittelt.

Natürlich führen Applikationen auch andere Dinge aus, als lediglich Daten mit Hilfe der CPU zu manipulieren. Diese können auch auf Benutzereingaben warten und genauso I/O zu Geräten ausführen, wie z.B. Laufwerken und Grafik-Displays. Wenn diese Ereignisse stattfinden, benötigt die Applikation die CPU nicht mehr länger. Dann kann die CPU dazu benutzt werden, andere Prozesse oder auch andere Applikationen laufen zu lassen, ohne die wartende Applikation dadurch zu verlangsamen.

Zusätzlich dazu kann die CPU bei einem anderen Konsumenten von Prozessleistung benutzt werden: dem Betriebssystem selbst.

3.2.2.2. Das Betriebssystem

Es ist schwierig festzustellen, wieviel Prozessleistung vom Betriebssystem selbst aufgebraucht wird. Betriebssysteme benutzen nämlich eine Mischung aus Prozess-Ebenen-Code und System-Ebenen-Code, um deren Arbeit durchzuführen. Während es zum Beispiel einfach ist, mittels Prozessüberwachung festzustellen, was der Prozess, der einen *daemon* oder *service* ausführt, gerade tut, ist es weniger einfach festzustellen, wieviel Prozessleistung bei I/O-bezogenen Abläufen auf System-Ebene aufgebraucht wird (was normalerweise innerhalb des Kontext des Prozesses geschieht, durch welchen I/O angefordert wird).

Generell ist es möglich, diese Art von Betriebssystem-Overhead in zwei Typen zu unterteilen:

- Betriebssystem Housekeeping
- Prozessbezogene Aktivitäten

Betriebssystem Housekeeping beinhaltet Aktivitäten, wie zum Beispiel Prozessplanung und Speicherverwaltung, wobei prozessbezogene Aktivitäten sämtliche Prozesse beinhalten, die das Betriebssystem selbst unterstützen, wie z.B. Prozesse, die systemweites Event-Logging oder I/O-Cache-Flushing abwickeln.

3.2.3. Verbessern eines CPU-Engpasses

Im Falle von unzureichender Prozessleistung für die Arbeit, welche erledigt werden muss, haben Sie zwei Optionen:

- Die Last reduzieren
- Die Kapazität erhöhen

3.2.3.1. Die Last reduzieren

Die CPU-Last zu reduzieren, kann auch ohne finanzielle Ausgaben erledigt werden kann. Der Trick dabei ist diejenigen Aspekte der Systemlast zu identifizieren, die sich in Ihrer Kontrolle befinden und die verringert werden können. Es gibt drei Bereiche, auf die man sich dabei konzentrieren muss:

- Betriebssystem-Overhead reduzieren
- Applikations-Overhead reduzieren
- Applikationen vollständig eliminieren

3.2.3.1.1. Betriebssystem-Overhead reduzieren

Um Betriebssystem-Overhead zu reduzieren, muss die gegenwärtige Systemlast überprüft werden und festgestellt werden, welche Aspekte zu ungewöhnlichen Overhead-Mengen führen. Dies könnte beinhalten:

- Den Bedarf nach häufiger Prozessplanung reduzieren
- Die Menge an geleistetem I/O reduzieren

Erwarten Sie keine Wunder. In einem einigermaßen gut konfigurierten System ist es unwahrscheinlich, dass eine große Leistungssteigerung beim Versuch Betriebssystem-Overhead zu reduzieren bemerkt wird. Dies ist damit erklärbar, dass ein einigermaßen gut konfiguriertes System, grundsätzlich nur ein minimale Menge an Overhead zur Folge hat. Wenn Ihr System jedoch z.B. mit zuwenig RAM ausgestattet ist, so kann Overhead reduziert werden, indem der RAM-Engpass ausgeglichen wird.

3.2.3.1.2. Applikations-Overhead reduzieren

Die Reduktion von Applikations-Overhead bedeutet gleichzeitig sicher zu gehen, dass die Applikation alles das besitzt, was diese zum einwandfreien Ablaufen benötigt. Manche Applikationen weisen absolut unterschiedliche Verhaltensweisen in verschiedenen Umgebungen auf — eine Applikation kann sich höchst compute-bound beim Verarbeiten bestimmter Arten von Daten verhalten, was z.B. bei anderen Daten wiederum nicht der Fall ist.

Dabei sollte im Auge behalten werden, dass Sie grundsätzlich ein gutes Verständnis der Applikationen besitzen müssen, die auf Ihrem System laufen, um diese so effizient als möglich ablaufen lassen zu können. Oft hat dies zur Folge, dass Sie mit Ihren Benutzern und/oder Entwicklern zusammenarbeiten müssen, um Wege herauszufinden, auf denen die Applikationen effizienter ablaufen können.

3.2.3.1.3. Applikationen vollständig eliminieren

Abhängig von Ihrem Unternehmen mag diese Vorgehensweise in Ihrem Fall nicht möglich sein, da es oft nicht im Verantwortungsbereich eines Systemadministrators liegt, vorzuschreiben welche Applikationen verwendet werden können und welche nicht. Wenn Sie jedoch Applikationen, welche als sogenannte "CPU-Hogs" (frei übersetzt als "CPU-Schweine") bekannt sind, ausfindig machen können, so können Sie vielleicht doch durchsetzen, dass von deren Verwendung abgesehen wird.

Diese Vorgehensweise involviert mit höchster Wahrscheinlichkeit nicht nur Sie selbst. Die betroffenen Benutzer sollten auch an diesem Prozess teilhaben dürfen, da diese in vielen Fällen das Wissen und das politische Durchsetzungsvermögen besitzen, um die notwendigen Änderungen in der Aufstellung der Applikationen durchzusetzen.

Tipp

Vergessen Sie dabei nicht, dass eine Applikation dabei nicht unbedingt von jedem System in Ihrem Unternehmen entfernt werden muss. Vielleicht sind Sie in der Lage eine speziell CPU-hungrige Applikation von einem überlasteten System zu einem System zu verschieben, welches kaum in Betrieb ist.

3.2.3.2. Erhöhen der Kapazität

Wenn es keine Möglichkeit gibt, die Nachfrage nach Prozessleistung zu reduzieren, dann sind Sie natürlich gezwungen, Wege und Mittel zu finden, wie bestehende Prozessleistung erhöht werden kann. Dies ist zwar mit Kosten verbunden, kann aber jederzeit durchgeführt werden.

3.2.3.2.1. Upgraden der CPU

Die einfachste Vorgehensweise ist festzustellen, ob Ihre System-CPU upgegraded werden kann. Der erste Schritt dabei ist festzustellen, ob die gegenwärtige CPU entfernt werden kann. Einige Systeme (vorwiegend Laptops) haben CPUs, welche angelötet sind, was ein Upgrade unmöglich macht. Der Rest besitzt jedoch gesockelte CPUs, was Upgrades möglich macht — zumindest in der Theorie.

Als nächstes müssen Sie ein paar Nachforschungen anstellen, ob eine schnellere CPU für Ihre Systemkonfiguration existiert. Wenn Sie zum Beispiel derzeit eine 1GHz CPU besitzen und eine 2GHz Einheit für den selben Typ existiert, so wäre ein Upgrade möglich.

Schlussendlich müssen Sie die maximale Taktrate feststellen, die von Ihrem System unterstützt wird. Um das obige Beispiel weiterzuführen, ist ein einfaches Austauschen der CPU nicht möglich, sollte Ihr System nur maximal 1 GHz Prozessoren unterstützen; auch wenn es eine passende 2GHz CPU gibt.

Sollten Sie keine schnellere CPU installieren können, so bestehen Ihre Möglichkeiten nur noch aus dem Austauschen von Hauptplatinen oder sogar dem bereits erwähnte und noch teureren 'Forklift'-Upgrade (gänzliches Austauschen des Computers).

Einige Systemkonfigurationen machen jedoch eine geringfügig andere Vorgangsweise möglich. Anstatt die jeweilige CPU zu ersetzen, warum nicht eine zweite CPU dazugeben?

3.2.3.2.2. Ist Symmetrisches Multiprocessing (Simultanverarbeitung) für Sie das Richtige?

Symmetrisches Multiprocessing (auch als SMP bekannt) macht es für ein Computersystem möglich, mehr als eine CPU zu besitzen, welche alle Systemressourcen gemeinsam benutzen. Dies bedeutet, dass im Gegensatz zu einem Uniprozessor-System auf einem SMP-System tatsächlich mehrere Prozesse zur selben Zeit ablaufen können.

Auf den ersten Blick scheint dies der Traum eines jeden Systemadministrators zu sein. Zuallererst macht es SMP möglich, die CPU-Leistung eines Systems zu erhöhen, auch wenn CPUs mit schnellerer Taktrate nicht erhältlich sind — und dies nur durch das Hinzufügen einer weiteren CPU. Jedoch kann diese Flexibilität auch Nachteile mit sich bringen.

Als Erstes sind nicht alle Systeme für SMP geeignet. Ihr System muss eine Hauptplatine besitzen, welches dazu ausgerichtet ist, mehrere Prozessoren zu unterstützen. Wenn dies nicht der Fall ist, so ist (zumindest) ein Hauptplatinen-Upgrade erforderlich.

Der zweiter Widerspruch ist der, dass SMP zur System-Overhead-Steigerung beiträgt. Es macht auch Sinn, wenn Sie kurz darüber nachdenken; mit mehreren CPUs, für die Arbeit geplant wird, benötigt das Betriebssystem logischerweise auch mehr CPU-Zyklen. Ein anderer Gesichtspunkt ist der, dass es mit mehreren CPUs auch mehr Auseinandersetzungen hinsichtlich der gemeinsam benutzten System-Ressourcen gibt. Deshalb resultiert das Upgraden eines Dual-Prozessor-Systems auf ein Quad-Prozessor-System auch nicht in einer 100prozentigen Steigerung der CPU-Leistungsfähigkeit. Tatsächlich ist es an einem bestimmten Punkt sogar möglich (abhängig von der eigentlichen Hardware, der Arbeitslast und der Prozessorarchitektur), dass durch das Hinzufügen eines weiteren Prozessors die Systemleistung sogar *verringert* wird.

Ein weiterer Punkt, den man dabei im Auge behalten sollte, ist dass SMP nicht hilfreich bei Arbeitslasten in Bezug auf eine monolithische Applikatio mit einer einzigen Ausführungssequenz ist. Wenn also z.B. ein großes Simulationsprogramm (höchst compute-bound) als ein Prozess ohne Threads abläuft, so läuft dieser Prozess nicht im Geringsten schneller auf einem SMP-System, als auf einer Einzel-Prozessor-Maschine ab. Tatsächlich kann dieser sogar etwas langsamer ablaufen, was auf den erhöhten Overhead durch SMP zurückzuführen wäre. Aus diesen Gründen entscheiden sich viele Systemadministratoren für eine Prozessleistung mit einem einzigen Ausführungsstrom, wenn es zum Thema CPU-Leistung kommt. Dies bietet die höchste CPU-Leistung und besitzt die wenigsten benutzungsbezogenen Einschränkungen.

Während diese Auseinandersetzung mit dem Thema möglicherweise den Anschein erweckt hat, dass SMP niemals eine gute Idee ist, gibt es Umstände, unter denen SMP sehr wohl Sinn macht. Umgebungen, auf denen mehrere Applikationen ablaufen, die sich höchst compute-bound verhalten, sind Anwärter für SMP. Der Grund dafür ist, dass Applikationen, die über lange Zeiträume hinweg nichts anderes tun als zu rechnen, dadurch die Auseinandersetzungen zwischen aktiven Prozessen (und deshalb auch den OS-Overhead) minimal halten, während der Prozess selbst jede CPU beschäftigt.

Ein weiterer Punkt, der in Hinblick auf SMP beachtet werden sollte, ist der Umstand, dass die Leistung weitaus eleganter mit steigenden Systemlasten sinkt, als dies ansonsten der Fall wäre. Dies macht SMP in Server und Multi-User Bereichen höchst populär, da der sich ständig ändernde Prozess-Mix auf einer Multi-Prozessormaschine weniger Auswirkungen auf die systemweite Auslastung hat.

3.3. Red Hat Enterprise Linux-spezifische Information

Zur Überwachung von Bandbreite und CPU-Auslastung unter Red Hat Enterprise Linux werden die in Kapitel 2 beschriebenen Tools benutzt. Sollten Sie dieses Chapter noch nicht gelesen haben, so raten wir Ihnen dringend an, dies noch bevor Sie fortfahren nachzuholen.

3.3.1. Überwachung von Bandbreite auf Red Hat Enterprise Linux

Wie in Abschnitt 2.4.2 erklärt, ist es schwierig Bandbreiten-Nutzung direkt zu überwachen. Durch die Prüfung von Device-Level-Statistiken ist es jedoch möglich grob abzuschätzen, ob ungenügende Bandbreite ein Problem auf Ihrem System darstellt.

Mit dem Befehl `vmstat` ist es möglich festzustellen, ob die allgemeine Geräte-Aktivität überhöht ist, indem Sie die Felder `bi` und `bo` dahingehend überprüfen. Die zusätzliche und genauere Betrachtung der Felder`si` und `so` gibt Ihnen mehr Einblick in Hinsicht auf Plattenaktivität, die durch Swap-bezogenen I/O entsteht:

```
   procs                      memory    swap          io     system         cpu
 r  b  w   swpd   free   buff  cache  si  so    bi    bo   in    cs  us  sy  id
```

```
 1  0  0      0 248088 158636 480804    0    0     2     6  120   120  10   3  87
```

In diesem Beispiel zeigt das `bi`-Feld an, dass zwei Blöcke pro Sekunde zu Block-Devicen geschrieben werden (hauptsächlich zu Laufwerken), während das `bo`-Feld sechs Blöcke pro Sekunde anzeigt, die von Block-Devicen gelesen wurden. Daraus können wir ersehen, dass keine dieser Aktivitäten auf Swapping zurückzuführen ist, da die `si` und `so`-Felder beide eine Swap-bezogene I/O-Rate von null Kilobytes/Sekunde anzeigen.

Durch die Benutzung von `iostat` ist es möglich, ein wenig mehr Einblick in Platten-bezogene Aktivität zu erhalten:

```
Linux 2.4.21-1.1931.2.349.2.2.entsmp (raptor.example.com)     07/21/2003

avg-cpu:  %user   %nice    %sys   %idle
           5.34    4.60    2.83   87.24

Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
dev8-0            1.10         6.21        25.08     961342    3881610
dev8-1            0.00         0.00         0.00         16          0
```

Dieser Output zeigt uns, dass der Durchschnitt für das Gerät mit Hauptnummer 8 (welches `/dev/sda`, die erste SCSI-Festplatte ist) nur geringfügig mehr als ein I/O Arbeitsgang pro Sekunde ist (das `tsp`-Feld). Der Grossteil der I/O-Aktivität für dieses Gerät ist auf Schreibvorgänge (das `Blk_wrtn`-Feld) mit geringfügig mehr als 25 Blöcken pro Sekunde zurückzuführen (das `Blk_wrtn/s`-Feld).

Für mehr Details benutzen Sie die `iostats -x`-Option:

```
Linux 2.4.21-1.1931.2.349.2.2.entsmp (raptor.example.com)     07/21/2003

avg-cpu:  %user   %nice    %sys   %idle
           5.37    4.54    2.81   87.27

Device:    rrqm/s wrqm/s   r/s   w/s  rsec/s  wsec/s    rkB/s    wkB/s avgrq-sz
/dev/sda    13.57   2.86  0.36  0.77   32.20   29.05    16.10    14.53    54.52
/dev/sda1    0.17   0.00  0.00  0.00    0.34    0.00     0.17     0.00   133.40
/dev/sda2    0.00   0.00  0.00  0.00    0.00    0.00     0.00     0.00    11.56
/dev/sda3    0.31   2.11  0.29  0.62    4.74   21.80     2.37    10.90    29.42
/dev/sda4    0.09   0.75  0.04  0.15    1.06    7.24     0.53     3.62    43.01
```

Nebst den längeren Zeilen, welche auch mehr Felder beinhalten, ist das Erste, das Sie im Auge behalten sollten, dass diese `iostat`-Ausgabe nunmehr Statistiken auf einer Pro-Partitions-Ebene aufzeigt. Wenn Sie `df` benutzen, um Mount-Punkte mit Gerätenamen zu verknüpfen, so ist es möglich diesen Report zu benutzen um festzustellen, ob zum Beispiel die Partition, welche `/home/` beinhaltet, einer überhöhten Arbeitsbelastung ausgesetzt ist.

Tatsächlich ist jede einzelne Zeilenausgabe von `iostat -x` länger und beinhaltet mehr Information als diese hier. Hier finden Sie den Rest jeder Zeile (mit der beigefügten Geräte-Spalte zum einfacheren Lesen):

```
Device:    avgqu-sz   await  svctm  %util
/dev/sda       0.24   20.86   3.80   0.43
/dev/sda1      0.00  141.18 122.73   0.03
/dev/sda2      0.00    6.00   6.00   0.00
/dev/sda3      0.12   12.84   2.68   0.24
/dev/sda4      0.11   57.47   8.94   0.17
```

In diesem Beispiel ist `/dev/sda2` interessanterweise die System Swap-Partition. Es ist offensichtlich, dass Swapping für diese Partition kein Problem auf diesem System ist, da viele Felder `0.00` anzeigen.

Ein weiterer interessanter Punkt ist `/dev/sda1`. Die Statistiken für diese Partition sind eher ungewöhnlich. Die allgemeine Aktivität scheint niedrig zu sein, wobei jedoch die durchschnittliche I/O-Anfragegröße (das `avgrq-sz`-Feld), die durchschnittliche Wartezeit (das `await`-Feld) und die durchschnittliche Servicezeit (das `svctm`-Feld) um einiges höher sind, als bei anderen Partitionen. Warum ist das so? Die Antwort darauf ist, dass diese Partition das `/boot/`-Verzeichnis beinhaltet, in dem Kernel und anfängliche Ramdisk gespeichert werden. Wenn das System bootet, so sind die Lese-I/Os (beachten Sie, dass nur die `rsec/s` und `rkB/s` nicht null sind; regelmäßig finden hier keine Schreibvorgänge statt), die während des Boot-Prozesses verwendet werden, für eine große Anzahl von Blöcken verantwortlich, was zu den relativ langen Warte- und Servicezeiten führt, welche in `iostat` angezeigt werden.

Es ist möglich den Befehl `sar` für einen Langzeitüberblick über I/O-Statistiken zu benutzen. Zum Beispiel kann mit `sar -b` ein allgemeiner I/O-Report angezeigt werden:

```
Linux 2.4.21-1.1931.2.349.2.2.entsmp (raptor.example.com)     07/21/2003

12:00:00 AM       tps      rtps      wtps   bread/s   bwrtn/s
12:10:00 AM      0.51      0.01      0.50      0.25     14.32
12:20:01 AM      0.48      0.00      0.48      0.00     13.32
...
06:00:02 PM      1.24      0.00      1.24      0.01     36.23
Average:         1.11      0.31      0.80     68.14     34.79
```

Hier, wie auch bei `iostat`s ursprünglicher Anzeige, sind die Statistiken für alle Block-Geräte gruppiert.

Ein anderer I/O-bezogener Report wird mittels dem Befehl `sar -d` erzeugt:

```
Linux 2.4.21-1.1931.2.349.2.2.entsmp (raptor.example.com)     07/21/2003

12:00:00 AM       DEV       tps    sect/s
12:10:00 AM    dev8-0      0.51     14.57
12:10:00 AM    dev8-1      0.00      0.00
12:20:01 AM    dev8-0      0.48     13.32
12:20:01 AM    dev8-1      0.00      0.00
...
06:00:02 PM    dev8-0      1.24     36.25
06:00:02 PM    dev8-1      0.00      0.00
Average:       dev8-0      1.11    102.93
Average:       dev8-1      0.00      0.00
```

Dieser Report beinhaltet eine Pro-Device-Information, jedoch mit wenigen Details.

Während es keine eindeutigen Statistiken zur Bandbreitennutzung für einen bestimmten Bus oder Datenpfad gibt, können wir jedoch zumindest feststellen, was die Devices tun und können deren Aktivitäten dazu benutzen, um indirekt die Bus-Beanspruchung festzustellen.

3.3.2. Überwachung der CPU-Nutzung auf Red Hat Enterprise Linux

Im Gegensatz zu Bandbreite ist das Überwachen von CPU-Nutzung ein überschaubares Thema. Vom prozentualen Anteil der CPU-Nutzung in **GNOME System Monitor** bis hin zu tiefgreifendeen Statistiken, dargestellt durch den `sar`-Befehl, ist es möglich genauestens festzustellen, wieviel CPU-Leistung verbraucht wird und wodurch.

Über den **GNOME System Monitor** hinaus, ist `top` das erste Ressource-Überwachungstool, das in Kapitel 2 behandelt wird und eine tiefgreifendere Darstellulng der CPU-Nutzung liefert. Hier ist ein `top`-Report von einem Dual-Prozessor-Arbeitsplatzgerät:

```
  9:44pm  up 2 days, 2 min,  1 user,  load average: 0.14, 0.12, 0.09
90 processes: 82 sleeping, 1 running, 7 zombie, 0 stopped
CPU0 states:  0.4% user,  1.1% system,  0.0% nice, 97.4% idle
CPU1 states:  0.5% user,  1.3% system,  0.0% nice, 97.1% idle
Mem:  1288720K av, 1056260K used,  232460K free,       0K shrd,  145644K buff
Swap:  522104K av,       0K used,  522104K free                  469764K cached

  PID USER     PRI  NI  SIZE  RSS SHARE STAT %CPU %MEM   TIME COMMAND
30997 ed        16   0  1100 1100   840 R     1.7  0.0   0:00 top
 1120 root       5 -10  249M 174M 71508 S <   0.9 13.8 254:59 X
 1260 ed        15   0 54408  53M  6864 S     0.7  4.2  12:09 gnome-terminal
  888 root      15   0  2428 2428  1796 S     0.1  0.1   0:06 sendmail
 1264 ed        15   0 16336  15M  9480 S     0.1  1.2   1:58 rhn-applet-gui
    1 root      15   0   476  476   424 S     0.0  0.0   0:05 init
    2 root      0K   0     0    0     0 SW    0.0  0.0   0:00 migration_CPU0
    3 root      0K   0     0    0     0 SW    0.0  0.0   0:00 migration_CPU1
    4 root      15   0     0    0     0 SW    0.0  0.0   0:01 keventd
    5 root      34  19     0    0     0 SWN   0.0  0.0   0:00 ksoftirqd_CPU0
    6 root      34  19     0    0     0 SWN   0.0  0.0   0:00 ksoftirqd_CPU1
    7 root      15   0     0    0     0 SW    0.0  0.0   0:05 kswapd
    8 root      15   0     0    0     0 SW    0.0  0.0   0:00 bdflush
    9 root      15   0     0    0     0 SW    0.0  0.0   0:01 kupdated
   10 root      25   0     0    0     0 SW    0.0  0.0   0:00 mdrecoveryd
```

Die erste CPU-bezogene Information befindet sich in der allerersten Zeile: die Durchschnittsbelastung. Die Durchschnittsbelastung ist eine Zahl, welche der durchschnittlichen Anzahl von ablaufenden Prozessen auf dem System entspricht. Der Belastungsdurchschnitt ist oft in Form von 3 Zahlen (wie bei `top`) aufgelistet, welche die Durchschnittsbelastung für die letzte Minute, die letzten fünf Minuten und 15 Minuten darstellen und in diesem konkreten Beispiel darauf hinweisen, dass das System nicht sehr ausgelastet war.

Die nächste Zeile, wenn auch nicht strikt auf CPU-Auslastung bezogen, besitzt einen indirekten Bezug, indem es die Anzahl der ablaufenden Prozesse (hier nur einer -- behalten Sie diese Zahl im Gedächtnis, da diese etwas Besonderes in diesem Beispiel bedeutet) anzeigt. Die Anzahl der ablaufenden Prozesse ist ein guter Indikator, wie CPU-bound ein System eventuell sein mag.

Als nächstes zeigen zwei Zeilen die gegenwärtige Auslastung für jede einzelne der beiden CPUs im System an. Die Nutzungsstatistiken sind aufgegliedert, um anzuzeigen, ob die CPU-Zyklen für Abläufe auf Benutzerebene oder Systemebene benutzt wurden; ebenso beinhaltet ist eine Statistik, die aufzeigt, wieviel CPU-Zeit von Prozessen mit abgeänderter Planungsdringlichkeit aufgebraucht worden ist. Schlussendlich finden Sie eine Idle-Time-Statistik (Zeit im Leerlauf).

Wenn wir uns hinunterbewegen zum Prozess-bezogenen Abschnitt der Anzeige, so sehen wir, dass der Prozess, der die meiste CPU-Leistung verbraucht `top` selbst ist; in anderen Worten war `top` der eine ablaufende Prozess auf diesem andererseits nicht produktiven System, der von sich selbst ein "Bild" gemacht hat.

Tipp

Es ist wichtig sich daran zu erinnern, dass in diesem Fall der eigentliche Überwachungsvorgang die von Ihnen erhaltenen Ressource-Nutzungsstatistiken beeinflusst. Dies trifft zu einem bestimmten Maße für jegliche Art von Überwachungssoftware zu.

Um detaillierteres Wissen über CPU-Nutzung zu erlangen, müssen wir mit anderen Tools arbeiten. Wenn wir die Ausgabe von `vmstat` überprüfen, so kommen wir zu einem geringfügig anderen Verständnis unseres Beispiel-Systems:

```
   procs                      memory    swap          io     system         cpu
 r  b  w   swpd   free   buff  cache  si  so    bi    bo   in    cs  us  sy  id
 1  0  0      0 233276 146636 469808   0   0     7     7   14    27  10   3  87
 0  0  0      0 233276 146636 469808   0   0     0     0  523   138   3   0  96
 0  0  0      0 233276 146636 469808   0   0     0     0  557   385   2   1  97
 0  0  0      0 233276 146636 469808   0   0     0     0  544   343   2   0  97
 0  0  0      0 233276 146636 469808   0   0     0     0  517    89   2   0  98
 0  0  0      0 233276 146636 469808   0   0     0    32  518   102   2   0  98
 0  0  0      0 233276 146636 469808   0   0     0     0  516    91   2   1  98
 0  0  0      0 233276 146636 469808   0   0     0     0  516    72   2   0  98
 0  0  0      0 233276 146636 469808   0   0     0     0  516    88   2   0  97
 0  0  0      0 233276 146636 469808   0   0     0     0  516    81   2   0  97
```

Hier haben wir den Befehl `vmstat 1 10` verwendet, um das System zehnmal hintereinander jede Sekunde abzufragen. Zuerst scheinen die CPU-bezogenen Statistiken (die `us`-, `sy`- und `id`-Felder) denjenigen zu gleichen, die von `top`angezeigt wurden, vielleicht sogar etwas weniger detailliert. Jedoch im Gegensatz zu `top` können wir ein wenig Einblick darin gewinnen, wie die CPU genutzt wird.

Wenn wir die `system`-Felder überprüfen, stellen wir fest, dass die CPU im Durchschnitt ungefähr 500 Interrupts pro Sekunde abwickelt und zwischen Prozessen irgendwo von 80 bis nahezu 400 mal pro Sekunde wechselt. Wenn Sie glauben, dass dies eine hohe Aktivität darstellt, dann denken Sie nochmals genau darüber nach. Die Abläufe auf Benutzerebene (das `us`-Feld) machen im Durchschnitt nur 2% aus, während Abläufe auf Systemebene (das `sy`-Feld) normalerweise unter 1% liegen. Nochmals, es handelt sich hier um ein nicht produktives System.

Bei nochmaliger Durchsicht der Sysstat-Tools zeigt sich, dass `iostat` und `mpstat` nur wenig zusätliche Informationen im Vergleich dazu bieten, was wir bereits durch `top` und `vmstat` festgestellt haben. `sar` produziert jedoch eine Anzahl von Reporten, die bei der Überwachung von CPU-Auslastung nützlich sein können.

Mit dem Befehl `sar -q` erhält man den ersten Report, welcher die Run-Queue-Länge darstellt sowie auch die Gesamtanzahl an Prozessen und die Belastung im Durchschnitt für die letzten 1 bis 5 Minuten. Hier ist ein Beispiel:

```
Linux 2.4.21-1.1931.2.349.2.2.entsmp (falcon.example.com)       07/21/2003

12:00:01 AM   runq-sz  plist-sz   ldavg-1   ldavg-5
12:10:00 AM         3       122      0.07      0.28
12:20:01 AM         5       123      0.00      0.03
...
09:50:00 AM         5       124      0.67      0.65
Average:            4       123      0.26      0.26
```

In diesem Beispiel ist das System immer beschäftigt (wenn man bedenkt, dass mehr als ein Prozess zu einem bestimmten Zeitpunkt ablaufen kann), jedoch nicht übermäßig belastet (aufgrund der Tatsache, dass dieses bestimmte System mehr als einen Prozessor besitzt).

Der nächste CPU-bezogene `sar`-Report wird durch den Befehl`sar -u` erstellt:

```
Linux 2.4.21-1.1931.2.349.2.2.entsmp (falcon.example.com)       07/21/2003

12:00:01 AM       CPU     %user     %nice   %system     %idle
12:10:00 AM       all      3.69     20.10      1.06     75.15
12:20:01 AM       all      1.73      0.22      0.80     97.25
```

```
...
10:00:00 AM       all     35.17      0.83      1.06     62.93
Average:          all      7.47      4.85      3.87     83.81
```

Die Statistiken, welche in diesem Report enthalten sind, unterscheiden sich nicht von denjenigen, die von vielen anderen Tools erstellt werden. Der größte Nutzen hierbei ist, dass `sar` die Daten auf fortlaufender Basis zur Verfügung stellt und daher besser geeignet zum Einholen von Langzeit-Durchschnittswerten ist oder auch für die Erstellung von CPU-Auslastungsdiagrammen.

Auf Multiprozessor-Systemen kann der `sar -U`-Befehl Statistiken für einen individuellen Prozessor oder auch für alle Prozessoren gleichzeitig erstellen. Hier ist ein Beispiel eines `sar -U ALL`-Output:

```
Linux 2.4.21-1.1931.2.349.2.2.entsmp (falcon.example.com)      07/21/2003

12:00:01 AM       CPU     %user     %nice   %system     %idle
12:10:00 AM         0      3.46     21.47      1.09     73.98
12:10:00 AM         1      3.91     18.73      1.03     76.33
12:20:01 AM         0      1.63      0.25      0.78     97.34
12:20:01 AM         1      1.82      0.20      0.81     97.17
...
10:00:00 AM         0     39.12      0.75      1.04     59.09
10:00:00 AM         1     31.22      0.92      1.09     66.77
Average:            0      7.61      4.91      3.86     83.61
Average:            1      7.33      4.78      3.88     84.02
```

Der Befehl `sar -w` erstellt einen Report über die Anzahl von Kontext-Switches pro Sekunde und gibt dabei zusätzlichen Einblick, wenn es darum geht wo CPU-Zyklen verbraucht werden:

```
Linux 2.4.21-1.1931.2.349.2.2.entsmp (falcon.example.com)      07/21/2003

12:00:01 AM   cswch/s
12:10:00 AM    537.97
12:20:01 AM    339.43
...
10:10:00 AM    319.42
Average:      1158.25
```

Es ist ebenso möglich, zwei verschiedene `sar`-Reporte über Interrupt-Aktivität zu erstellen. Der erste Report (mittels `sar -I SUM`-Befehl erstellt) zeigt eine einzige "Interrupts pro Sekunde"-Statistik an:

```
Linux 2.4.21-1.1931.2.349.2.2.entsmp (falcon.example.com)      07/21/2003

12:00:01 AM      INTR    intr/s
12:10:00 AM       sum    539.15
12:20:01 AM       sum    539.49
...
10:40:01 AM       sum    539.10
Average:          sum    541.00
```

Durch das Benutzen des Befehls `sar -I PROC` ist es möglich Interrupt-Aktivität in Prozessoren aufzuschlüsseln (auf Multiprozessor-Systemen) *und* in Interrupt-Ebenen (von 0 bis 15):

```
Linux 2.4.21-1.1931.2.349.2.2.entsmp (pigdog.example.com)      07/21/2003

12:00:00 AM  CPU  i000/s  i001/s  i002/s  i008/s  i009/s  i011/s  i012/s
12:10:01 AM    0  512.01    0.00    0.00    0.00    3.44    0.00    0.00
```

```
12:10:01 AM  CPU  i000/s  i001/s  i002/s  i008/s  i009/s  i011/s  i012/s
12:20:01 AM    0  512.00    0.00    0.00    0.00    3.73    0.00    0.00
...
10:30:01 AM  CPU  i000/s  i001/s  i002/s  i003/s  i008/s  i009/s  i010/s
10:40:02 AM    0  512.00    1.67    0.00    0.00    0.00   15.08    0.00
Average:       0  512.00    0.42    0.00     N/A    0.00    6.03     N/A
```

Dieser Report (welcher horizontal abgeschnitten wurde, um auf diese Seite zu passen) beinhaltet eine Rubrik für jede Interrupt-Ebene (wie zum Beispiel das `i002/s`-Feld, das die Rate für Interrupt-Ebene 2 darstellt). Wenn dies ein Multiprozessor-System wäre, dann gäbe es eine Zeile pro Beispiel-Periode für jede einzelne CPU.

Beachten Sie auch bei diesem Report, dass von `sar` spezifische Interrupt-Felder entweder hinzufügt oder entfernt werden, wenn keine Daten für dieses Feld gesammelt werden. Der oben angefürte Report stellt dahingehend ein Beispiel zur Verfügung, indem dieser am Ende Interrupt-Ebenen (3 und 10) beinhaltet, die zu Beginn der Abfrageperiode nicht vorhanden waren.

Anmerkung

Es gibt noch zwei andere Interrupt-bezogene `sar`-Reporte — `sar -I ALL` und `sar -I XALL`. Jedoch sammelt die standardmäßige Konfiguration für `sadc` nicht die notwendige Information für diese Reporte. Dies kann durch das Bearbeiten der Datei `/etc/cron.d/sysstat` geändert werden, indem diese Zeile verändert wird:

```
*/10 * * * * root /usr/lib/sa/sa1 1 1
```

Zu dieser:

```
*/10 * * * * root /usr/lib/sa/sa1 -I 1 1
```

Beachten Sie dabei, dass diese Änderung die Sammlung zusätzlicher Informationen im Falle von `sadc` und dies gleichzeitig größere Dateigrößen zur Folge hat. Stellen Sie daher sicher, dass Ihre Systemkonfiguration den zusätzlichen Verbrauch von Platz unterstützt.

3.4. Zusätzliche Ressourcen

Dieser Abschnitt beinhaltet verschiedenste Ressourcen, die dazu verwendet werden können mehr über die Red Hat Enterprise Linux-spezifischen Themen zu lernen, die in diesem Kapitel behandelt wurden.

3.4.1. Installierte Dokumentation

Die folgenden Ressourcen wurden im Laufe einer typischen Red Hat Enterprise Linux-Installation installiert und helfen Ihnen mehr über die behandelten Gegenstände in diesem Kapitel zu lernen.

- `vmstat(8)` man-Seite — Lernen Sie, wie Sie einen präzisen Überblick über Prozess, Speicher, Swap, I/O, System und CPU-Nutzung bekommen.
- `iostat(1)` man-Seite — Lernen Sie CPU- und I/O-Statistiken anzuzeigen.
- `sar(1)` man-Seite — Lernen Sie System-Ressourcen-Nutzungsreporte zu erstellen.
- `sadc(8)` man-Seite — Lernen Sie System-Nutzungsdaten zu sammeln.

- `sa1(8)` man-Seite — Lernen Sie mehr über ein Script, das `sadc` periodisch ablaufen lässt.
- `top(1)` man-Seite — Lernen Sie CPU-Nutzungs- und Prozessebenen-Statistiken anzeigen zu lassen.

3.4.2. Nützliche Webseiten

- http://people.redhat.com/alikins/system_tuning.html — System-Tuning-Info für Linux Server. Eine gewissenhafte Betrachtungsweise von Performance-Tuning und Ressourcenkontrolle für Server.
- http://www.linuxjournal.com/article.php?sid=2396 — Leistungskontrolle-Tools für Linux. Diese Linux Journalseite ist mehr für den Administrator ausgerichtet, der daran interessiert ist, eine maßgeschneiderte Performance-Graphing-Lösung zu schreiben. Da bereits einige Jahre vergangen sind, seit dieser Artikel verfasst worden ist, besteht die Möglichkeit, dass einige Details nicht mehr länger zutrefffen. Generell gesehen sind jedoch das darin enthaltene Gesamtkonzept und die entsprechende Ausführung einwandfrei.

3.4.3. Bücher zum Thema

Die folgenden Bücher behandeln verschiedenste Themen zur Ressourcenkontrolle und stellen gute literarische Quellen für Red Hat Enterprise Linux-Systemadministratoren dar:

- *Red Hat Enterprise Linux Handbuch zur System-Administration*; Red Hat, Inc. — Beinhaltet ein Kapitel über viele der hier beschriebenen Ressourcenkontrolle-Tools.
- *Linux Performance Tuning and Capacity Planning* von Jason R. Fink und Matthew D. Sherer; Sams — Liefert einen detaillierteren Überblick über die hier vorgestellten Ressourcenkontrolle-Tools und beinhaltet ebenso andere Tools, die für spezifischere Zwecke der Ressourcenkontrolle ebenfalls geeignet sein könnten.
- *Linux Administration Handbook* von Evi Nemeth, Garth Snyder und Trent R. Hein; Prentice Hall — Liefert ein kurzes Kapitel in ähnlichem Rahmen als dieses Buch, beinhaltet jedoch zusätzlich einen interessanten Abschnitt zur Diagnose eines Systems, das plötzlich langsamer geworden ist.
- *Linux System Administration: A User's Guide* von Marcel Gagne; Addison Wesley Professional — Beinhaltet ein kurzes Kapitel bezüglich Leistungskontrolle und Tuning.

Kapitel 4.

Physikalischer und virtueller Speicher

Alle modernen, allgemein verwendeten Computer sind auch als *Stored Program Computers* oder speicherprogrammierte Rechner bekannt. Wie der Name besagt, laden speicherprogrammierte Computer Anweisungen (die Blöcke eines Programms) in einen internen Speicher, wo diese Anweisungen dann ausgeführt werden.

Diese Computer verwenden den gleichen Speicher auch für Daten. Dies steht im Gegensatz zu Computern, die ihre Hardware-Konfiguration zur Steuerung des Betriebs verwenden (z.B. ältere Steckbrett-basierte Computer).

Der Ort, wo Programme auf den ersten speicherprogrammierten Computern gespeichert wurden, war unter zahlreichen Namen bekannt und benutzte zahlreiche unterschiedliche Technologien, die von Punkten auf einer Elektronenstrahlröhre bis hin zu Druckimpulsen in Quecksilbersäulen reichten. Glücklicherweise benutzen Computer heutzutage Technologien mit einer größeren Speicherkapazität und einem kleineren Format als jemals zuvor.

4.1. Zugriffsmuster auf Speicher

Was Sie jedoch durchwegs beachten sollten, ist die Tatsache, dass Computer in einer bestimmten Art auf Speicher zugreifen. Tatsächlich besitzen die meisten Speicherzugriffe eines (oder beide) der folgenden Attribute:

- Zugriff neigt dazu sequentiell zu sein
- Zugriff neigt dazu ortsgebunden zu sein

Sequentieller Zugriff bedeutet, dass wenn auf Adresse N von der CPU zugegriffen wird, es höchstwahrscheinlich ist, dass auf die Adresse N+1 als nächstes zugegriffen wird. Dies macht dadurch Sinn, dass die meisten Programme aus großen Instruktionsabschnitten bestehen, die — der Reihenfolge nach — ausgeführt werden.

Lokaler Zugriff bedeutet, dass wenn auf Adresse X zugegriffen wird, dass auf andere Adressen, die X umgeben, in Zukunft auch zugegriffen wird.

Diese Attribute sind äußerst wichtig, da es kleinerem, schnellerem Speicher ermöglicht, größeren, langsameren Speicher gewissermaßen zu puffern. Bevor wir jedoch virtuellen Speicher genauer betrachten, müssen wir dazu die verschiedenen Speichertechnologien, die derzeit benutzt werden, genauer unter die Lupe nehmen.

4.2. Das Speicherspektrum

Moderne Computer benutzen tatsächlich eine Vielzahl von Speichertechnologien. Jede Technologie ist mit entsprechenden Geschwindigkeiten und Speicherkapazitäten auf eine spezielle Funktion hin ausgerichtet.

Die Technologien sind:

- CPU-Register
- Cache-Speicher
- RAM
- Festplatten

- Offline-Backupspeicher (Band, Optische Disk, usw.)

Hinsichtlich Leistungsvermögen und Kosten gibt es ein breites Spektrum dieser Technologien. CPU-Register zeichnet zum Beispiel folgendes aus:

- Sehr schnell (Zugriffszeiten von einigen Nanosekunden)
- Niedrige Kapazität (gewöhnlich weniger als 200 Bytes)
- Sehr eingeschränktes Erweiterungsvermögen (eine Veränderung in der CPU-Architektur wäre notwendig)
- Teuer (mehr als ein Dollar/Byte)

Hingegen am anderen Ende des Spektrums befinden sich die Offline-Backupspeicher:

- Sehr langsam (Zugriffszeiten werden eventuell in Tagen gemessen, falls das Speichermedium über weite Entfernungen versandt werden muss)
- Sehr hohe Kapazität (1/10 - 1/100 eines Gigabyte)
- Im Wesentlichen ein grenzenloses Erweiterungsvermögen (lediglich durch die Räumlichkeiten begrenzt, die zum Aufbewahren des Backup-Mediums selbst notwendig sind)
- Sehr kostengünstig (Bruchteile von Cents/Byte)

Durch die Benutzung verschiedener Technologien mit verschiedenen Leistungsfähigkeiten ist es möglich, ein Systemdesign so abzustimmen, dass die maximale Leistungsfähigkeit bei geringstmöglichem Kostenaufwand erreicht wird. Die folgenden Abschnitte befassen sich näher mit jeder Art von Technologie im Speicherspektrum.

4.2.1. CPU-Register

Jedes heutige CPU-Design beinhaltet Register für eine Vielzahl von Zwecken. Diese reichen vom Speichern der Adresse der gegenwärtig ausgeführten Instruktion bis hin zu mehr allgemeiner Datenspeicherung und Datenbearbeitung. CPU-Register laufen in der selben Geschwindigkeit ab, wie der Rest der CPU; ansonsten wären diese ein ernstzunehmender Engpass in der allgemeinen Systemleistung. Der Grund dafür ist, dass nahezu alle Abläufe der CPU auf die eine oder andere Weise auch die Register miteinbeziehen.

Die Anzahl der CPU-Register (und deren Verwendungszweck) hängen von der Architektur der CPU ab. Es ist keinesfalls möglich, die Anzahl der CPU-Register zu verändern, außer Sie wechseln zu einer CPU mit einer anderen Architektur. Aus diesen Gründen kann die Anzahl der CPU-Register als Konstante angesehen werden, da diese nur unter großem Aufwand, auch in finanzieller Hinsicht, ausgetauscht werden können.

4.2.2. Cache-Speicher

Cache-Speicher oder auch Pufferspeicher genannt, arbeiten wie ein Puffer zwischen den sehr eingeschränkten, Hochgeschwindigkeits-CPU-Registern und dem relativ langsameren und wesentlich größeren Haupt-Systemspeicher — normalerweise auch als RAM bezeichnet[1]. Cache-Speicher besitzten eine Betriebsgeschwindigkeit, die ähnlich der CPU-Betriebsgeschwindigkeit ist. Dies bedeutet, dass wenn die CPU auf Daten im Cache zugreift, muss die CPU nicht erst auf die Daten warten.

Cache-Speicher werden dahingehend konfiguriert, dass wann auch immer Daten von RAM gelesen werden sollen, die Systemhardware zuallererst überprüft, ob die gewünschten Daten sich im Cache

1. Während "RAM" ein Akronym ist für "Random Access Memory" und eine Bezeichnung die nahezu auf jede Speichertechnologie zutreffen könnte, die nicht-sequentiellen Zugriff auf gespeicherte Daten ermöglicht. Wenn Systemadministratoren jedoch von RAM sprechen, dann meinen diese ausnahmslos den Haupt-Systemspeicher.

befinden. Wenn sich die gesuchten Daten im Cache befinden, dann kann auf diese rasch zugegriffen werden und diese können von der CPU benutzt werden. Sollten sich die Daten jedoch nicht im Cache befinden, so werden die Daten direkt vom Hauptspeicher bezogen und während deren Übertragung an die CPU ebenfalls im Cache gespeichert (für den Fall, dass diese später nochmals benötigt werden). Aus der Sicht der CPU macht es grundsätzlich keinen Unterschied, ob auf Daten im Cache oder im RAM zugegriffen wird, mit Ausnahme der unterschiedlichen Zugriffsgeschwindigkeit.

In Hinsicht auf Speicherkapazität ist Cache dem RAM um einiges unterlegen. Deshalb kann nicht jeder Byte im RAM seinen eigenen einzigartigen Platz im Cache besitzen. Es ist daher notwendig Cache in Sektionen aufzugliedern, die zum Zwischenspeichern verschiedener Bereiche im RAM verwendet werden können. Ebenso wird ein spezieller Mechanismus benötigt, welcher jedem Cache-Bereich erlaubt, verschiedene Bereiche des RAM zu verschiedenen Zeiten zwischenzuspeichern. Trotz des Unterschiedes in Speicherkapazität und angesichts der sequentiellen und örtlich begrenzten Natur des Speicherzugriffs kann eine geringe Menge an Cache auf höchst effektive Art und Weise den Zugang zu einer großen Menge an RAM beträchtlich beschleunigen.

Wenn Daten von der CPU geschrieben werden, dann kann es allerdings etwas komplizierter werden. Es gibt zwei Arten der Durchführung. In beiden Fällen werden die Daten zuerst in den Cache geschrieben. Da jedoch der Hauptzweck von Cache die Funktion des sehr schnellen Kopierens von Inhalten ausgewählter Teile des RAM ist, so muss jede auch noch so geringe Datenänderung im RAM und im Cache gespeichert werden. Ansonsten würden die Daten im RAM nicht mehr länger mit den Daten im Cache übereinstimmen.

Die beiden verschiedenen Arten unterscheiden sich in deren Durchführung. Eine Art, auch als *Write-Through*-Caching bekannt, schreibt die modifizierten Daten umgehend in den RAM-Speicher. *Write-Back*-Caching verzögert jedoch das Schreiben der modifizierten Daten in RAM. Hauptgrund dafür ist die Reduktion der Häufigkeit des RAM-Speichervorganges im Falle von häufig modifizieren Daten.

Ein Write-Through-Cache ist ein wenig einfacher zu implementieren; aus diesem Grund auch häufiger anzutreffen. Write-Back-Cache ist ein wenig schwieriger zu implementieren; zusätzlich zum Speichern der aktuellen Daten ist es notwendig, eine Art Mechanismus aufrecht zu erhalten, der die Daten im Cache als 'clean' flagged (Daten im Cache entsprechen genau den Daten im RAM) oder auch als 'dirty' (Daten im Cache wurden modifiziert, was bedeutet, dass die Daten im Hauptspeicher nicht mehr länger aktuell sind). Es ist ebenso notwendig einen Ablauf zu implementieren, der garantiert, dass in bestimmten Abständen 'dirty' Cache-Einträge zum Hauptspeicher zurück-"geflushed" werden.

4.2.2.1. Cache-Levels

Cache-Subsysteme können in modernen Computerarchitekturen auch multi-level sein; was soviel bedeutet, als dass es auch mehr als ein Cache-Set zwischen der CPU und dem Hauptspeicher geben kann. Die Cache-Level sind oft nummeriert, wobei die niedrigeren Nummern meist näher an der CPU sind. Viele Systeme besitzen zwei Cache-Level:

- Der L1-Cache befindet sich oft direkt auf dem CPU-Chip und besitzt die selbe Geschwindigkeit als die CPU
- Der L2-Cache ist oft ein Teil des CPU-Moduls, läuft mit CPU-Geschwindigkeit ab (oder beinahe) und ist für gewöhnlich ein wenig größer und langsamer als der L1-Cache.

Einige Systeme (normalerweise Hochleistungsserver) besitzen auch einen L3-Cache, welcher normalerweise ein Teil der System-Hauptplatine ist. Wie höchstwahrscheinlich angenommen wird, würde der L3-Cache größer (und höchstwahrscheinlich langsamer) als der L2-Cache sein.

In jedem Fall ist die Zielsetzung aller Cache-Subsysteme — egal ob Einzel- oder Multi-Level-System — die durchschnittliche Zugriffszeit auf den Hauptspeicher zu reduzieren.

4.2.3. Hauptspeicher — RAM

RAM (Random Access Memory/Speicher mit beliebigem Zugriff) macht den Großteil an elektronischem Speicher in heutigen Computern aus. RAM wird als Speicher für sowohl Daten, als auch Programme benutzt, während diese Daten und Programme benutzt werden. Die RAM-Geschwindigkeit liegt heutzutage bei den meisten Computern irgendwo zwischen der Cache- und Festplatten-Geschwindigkeit, jedoch etwas näher an der Cache-Geschwindigkeit.

Der grundsätzliche Betrieb von RAM ist eigentlich ziemlich einfach. An unterster Stufe gibt es die sogenannten RAM-Chips (Chip-Bausteine) — integrierte Schaltkreise, welche für das eigentliche "Erinnern" zuständig sind. Diese Chips besitzen vier Arten von Verbindungen zur Außenwelt.

- Stromanschluss (um die Schaltung innerhalb des Chip zu betreiben)
- Datenverbindungen (um den Datentransfer in oder aus dem Chip zu ermöglichen)
- Schreib-/Lesezugriffe (um zu kontrollieren, ob Daten entweder im Chip gespeichert werden sollen oder von dort wieder abgerufen)
- Adressenverbindungen (um festzustellen, wo im Chip die Daten gelesen/geschrieben werden sollten)

Hier sind die notwendigen Schritte, um Daten im RAM zu speichern:

1. Die zu speichernden Daten werden den Datenverbindungen vorgelegt.
2. Die Adresse, an der die Daten gespeichert werden sollen wird den Adressenverbindungen vorgelegt.
3. Die Lese-/Schreibverbindung ist auf Schreibmodus gesetzt.

Das Abrufen von Daten läuft genauso einfach ab:

1. Die Adresse der gewünschten Daten wird den Adressenverbindungen vorgelegt.
2. Die Lese-/Schreibverbindung ist auf Lesemodus gesetzt.
3. Die gewünschten Daten werden von den Datenverbindungen gelesen.

Während diese Schritte simpel erscheinen, finden diese in sehr hohen Geschwindigkeiten statt, wobei die Zeit jeden Schrittes in Nanosekunden gemessen wird.

Beinahe alle RAM-Chips, die heutzutage erzeugt werden, werden als *Module* zusammengefasst. Jedes Modul besteht aus einer Anzahl von individuellen RAM-Chips, die an einer kleinen Platine angebracht sind. Die mechanische und elektrische Anordnung der Module hält verschiedenste Industrie-Standards ein und macht es daher möglich, Speicher von verschiedensten Herstellern zu beziehen.

Anmerkung

Der Hauptvorteil eines Systems, welches industriestandardisierte RAM-Module benutzt, ist der niedrige Kostenfaktor, da Module von mehr als einem Hersteller und nicht nur dem Systemhersteller selbst bezogen werden können.

Obwohl die meisten Computer Industrie-standardisierte RAM-Module verwenden, gibt es noch Ausnahmen. Am meisten sind dabei Laptops (und sogar hier tritt bereits eine Art Standardisierung ein) und High-End-Server zu beachten. Jedoch ist es auch unter diesen Umständen höchstwahrscheinlich möglich, RAM-Module von anderen Herstellern zu bekommen, wenn es sich dabei um ein relativ populäres System und nicht ein komplett neues Design handelt.

4.2.4. Festplatten

Sämtliche bisher behandelten Technologien sind von Natur aus *volatil*. In anderen Worten gehen Daten, die in volatilen Speichern vorhanden sind, beim Ausschalten des PCs verloren.

Festplatten sind jedoch *nicht-volatil* — Die Daten, welche diese enthalten gehen nicht beim Ausschalten des PCs oder bei einer Unterbrechung der Stromzufuhr verloren. Deshalb nehmen Festplatten einen ganz speziellen Platz im Speicher-Spektrum ein. Deren nicht-volatile Eigenschaft macht diese zum idealen Medium, um Programme und Daten für den Langzeitgebrauch zu speichern. Ein anderer und auch einzigartiger Aspekt von Festplatten ist die Tatsache, dass Programme nicht wie bei RAM und Cache direkt ausgeführt werden können. Stattdessen müssen diese zuerst in den Hauptspeicher eingelesen werden.

Auch unterscheidet sich die Geschwindigkeit der Datenablage und -abfrage im Vergleich zu RAM und Cache; Festplatten sind mindestens eine Größenordnung langsamer, als die vollelektronischen Technologien, die für RAM und Cache verwendet werden. Der Unterschied in Geschwindigkeit liegt hauptsächlich in deren elektro-mechanischer Natur. Es gibt vier eindeutige Phasen, die während jedes Datentransfers von oder zu derFestplatte durchlaufen werden. Die folgende Auflistung veranschaulicht diese Phasen, gemeinsam mit der Zeit, die von jedertypischen Hochleistungsplatte benötigt werden würde, um jede einzelne dieser Phasen zu durchlaufen:

- Zugriffs-Positionierzeit (5,5 Millisekunden)
- Plattendrehzahl (0,1 Millisekunden)
- Datenbearbeitung durch Lese-/Schreibköpfe (0,00014 Millisekunden)
- Datenübernahme und/oder Datenübertragung von/zur Elektronik der Festplatte (0,003 Millisekunden)

Lediglich die letzte Phase ist unabhängig von irgendeinem mechanischen Verfahren.

Anmerkung

Obwohl es noch viel mehr über Festplatten zu lernen gibt, werden Festplattenspeichertechnologien genauer in Kapitel 5 behandelt. Einstweilen ist es nur notwendig den hohen Geschwindigkeitsunterschied zwischen RAM und Festplatten-basierten Speichern im Gedächtnis zu behalten und dass deren Speicherkapazität die von RAM für gewöhnlich um mindestens das Zehnfache und oft auch um das Hunderfache und mehr übersteigt.

4.2.5. Offline-Datensicherungsspeicher (Offline-Backup-Speicher)

Offline-Datensicherungsspeicher besitzen eine höhere Kapazität, sind jedoch langsamer. Hierbei ist die Kapazität lediglich durch das Vorhandensein von Lagerplätzen für die entfernbaren Speichermedien eingeschränkt.

Die tatsächlichen Technologien, welche in den Geräten verwendet werden variieren sehr stark. Hier finden Sie die gängigsten Typen:

- Magnetband
- Optische Disk

Logischerweise sind die Zugriffszeiten bei entfernbaren Speichermedien höher. Dies ist vor allem dann der Fall, wenn die gewünschten Daten sich auf einem Datenträger befinden, der zu diesem Zeitpunkt noch nicht in das Speichergerät geladen worden ist. Diese Situation wird durch die Benutzung

von Device-Robotern erleichtert, welche das automatische Laden und Entladen von Medien durchführen können, wobei die Speicherkapazitäten solcher Geräte noch immer begrenzt sind. Selbst im besten Fall werden Zugriffszeiten in Sekunden bemessen, welche vergleichsweise wesentlich höher sind als die relativ langsamen in Multi-Millisekunden gemessenen Zugriffszeiten, welche typisch für eine Hochleistungs-Festplatte sind.

Da wir nunmehr kurz die verschiedenen Speichertechnologien, die heutzutage verwendet werden, duchgegangen sind, widmen wir uns nun den grundlegenden Konzepten von virtuellem Speicher.

4.3. Grundlegende Konzepte virtuellen Speichers

Obwohl die Technologie, die sich heutzutage hinter den verschiedensten modernen Speichertechnologien verbirgt, schlichtweg eindrucksvoll ist, muss der durchschnittliche Systemadministrator sich nicht näher mit den Details befassen. Tatsächlich gibt es nur eine Tatsache, die Systemadministratoren in Bezug auf Speicher immer im Gedächtnis behalten sollten:

Es gibt niemals genug RAM.

Während diese Binsenweisheit zunächst sehr humorvoll erscheinen mag, so haben zahlreiche Designer von Betriebssystemen geraume Zeit damit verbracht, die Auswirkungen dieses sehr realen Engpasses zu verringern. Dies wurde bewerkstelligt durch die Implementierung *virtuellen Speichers* — eine Art Kombination von RAM mit langsamerem Speicher, um dem System den Anschein zu geben, mehr RAM zu besitzen, als eigentlich installiert worden ist.

4.3.1. Virtueller Speicher in einfachen Worten

Beginnen wir mit einer hypothetischen Applikation. Der Maschinencode, aus dem diese Applikation besteht, besitzt eine Größe von 10000 Bytes. Außerdem werden weitere 5000 Bytes zur Datenspeicherung und für I/O-Puffer benötigt. Dies bedeutet, dass diese Applikation 15000 Bytes RAM benötigt; sogar bei einem einzigen Byte weniger könnte die Applikation nicht ablaufen.

Diese Voraussetzung von 15000 Byte ist auch als *Adressbereich* der Applikation bekannt. Es stellt die Anzahl von einzigartigen Adressen dar, die dazu benötigt werden, die Applikation und deren Daten zu enthalten. In den ersten Computern musste der Adressbereich größer sein, als der Adressbereich der größten Applikation, die darauf ablaufen sollte; ansonsten würde die Applikation fehlschlagen und eine "Out of Memory"-Fehlermeldung ("Speicher unzureichend") erzeugen.

Eine spätere Vorgehensweise, als *Overlaying* bekannt, versuchte das Problem zu verringern, indem Programmierer festlegen konnten, welche Teile derer Applikationen im Speicher zu jedem gegebenen Zeitpunkt resident bleiben. Auf diese Art konnte Code, der nur einmalig zu Initialisierungszwecken benötigt wird, mit Code überschrieben (overlayed) werden, der zu einem späteren Zeitpunkt benötigt wird. Während Overlays im Falle von Speicherknappheit Erleichterung schaffen konnten, so war dies jedoch ein sehr komplexer und fehleranfälliger Prozess. Overlays haben auch nicht das Problem einer systemweiten Speicherknappheit während der Laufzeit angesprochen. In anderen Worten erfordert ein Programm mit Overlays zwar weniger Speicher zum Ablaufen, besitzt das System jedoch nicht genügend Speicher für das darübergelegte (overlayed) Programm, bleibt das Endresultat unverändert — eine "Out of Memory"-Fehlermeldung.

Virtueller Speicher stellt das Konzept eines Adressbereichs für Applikationen auf den Kopf. Anstatt sich darauf zu konzentrieren, *wieviel* Speicher eine Applikation zum Ablaufen benötigt, versucht ein Betriebssystem mit virtuellem Speicher ständig die Antwort auf eine Frage zu finden, nämlich "*wiewenig* Speicher benötigt eine Applikation zum Ablaufen?"

Wobei es zunächst danach aussieht, als ob unsere hypothetische Applikation die gesamten 15000 Bytes zum Ablaufen benötigt, bitten wir Sie, sich an unsere Diskussion zurückzuerinnern in Abschnitt 4.1 — Speicherzugriff neigt dazu, sequentiell und ortsgebunden zu sein. Daher ist die Menge an benötigtem Speicher (um die Applikation auszuführen) zu jedem Zeitpunkt weniger als 15000 Bytes

— normalerweise sogar um Einiges weniger. Betrachten Sie die Arten von Speicherzugriffen, die notwendig sind, um einen einzigen Maschinenbefehl auszuführen:

- Der Befehl wird vom Speicher gelesen.
- Die Daten, die vom Befehl benötigt werden, werden vom Speicher gelesen.
- Nachdem der Befehl durchgeführt worden ist, werden die Resultate des Befehls wieder zurück in den Speicher geschrieben.

Die eigentliche Menge von Bytes, die für jeden Speicherzugriff notwendig sind, variiert in Hinsicht auf CPU-Architektur, den tatsächlichen Befehl und den Datentyp. Selbst wenn ein Befehl 100 Bytes für jede Art von Speicherzugang benötigt, so sind die benötigten 300 Bytes immer noch viel niedriger als der gesamte 15000-Byte Adressbereich der Applikation. Wenn es eine Möglichkeit gäbe, die Speicheranforderungen einer Applikation nachzuverfolgen während diese abläuft, so wäre es möglich die Applikation auch mit weniger Speicher, als vom Adressbereich gefordert, ablaufen zu lassen.

Da bleibt nur noch eine Frage übrig:

Wenn nur ein Teil der Applikation sich zu einem bestimmten Zeitpunkt im Speicher befindet, wo befindet sich der Rest?

4.3.2. Zusatzspeicher — zentraler Grundsatz des virtuellen Speichers

Kurz gesagt verbleibt der Rest der Applikation auf der Festplatte. In anderen Worten fungiert die Festplatte als *Zusatzspeicher* für RAM; ein langsameres, größeres Speichermedium dient als "Backup" für ein viel schnelleres, kleineres Speichermedium. Dies mag zunächst den Eindruck eines großen Performance-Problems in spe erwecken — sind doch Festplattenlaufwerke um so vieles langsamer als RAM.

Während dies der Wahrheit entspricht, ist es jedoch möglich seine Vorteile aus dem sequentiellen und ortsgebundenen Zugriffsverhalten von Applikationen zu ziehen und die meisten negativen Auswirkungen auf die Leistung zu elimieren, sobald Festplattenlaufwerke als Zusatzspeicher für den Hauptspeicher verwendet werden. Das Subsystem des virtuellen Speichers wird dahingehend strukturiert, dass dieses versucht sicherzustellen, dass diejenigen Teile der Applikation, die sich gerade in Gebrauch befinden oder höchstwahrscheinlich in naher Zukunft benötigt werden, für den benötigten Zeitraum lediglich in RAM aufbewahrt werden.

In vieler Hinsicht ist dies ähnlich der Beziehung zwischen Cache und RAM: indem ein kleiner, schneller Speicher gemeinsam mit einem großen, langsamen Speicher sich wie eine große Menge schneller Speicher verhalten.

In Anbetracht dessen, sehen wir uns den Prozess nun einmal genauer an.

4.4. Virtueller Speicher: Die Details

Zunächst müssen wir ein neues Konzept vorstellen: *virtueller Adressbereich*. Virtueller Adressbereich ist die maximale Menge an Adressbereich, der einer Applikation zur Verfügung steht. Der virtuelle Adressbereich variiert entsprechend der Systemarchitektur und ist abhängig vom Betriebssystem. Virtueller Adressbereich hängt von der Architektur ab, da die Architektur genau bestimmt wieviele Bits zu diesem Zweck zur Verfügung stehen. Virtueller Speicherraum hängt ebenso vom Betriebssystem ab, da die Art in welcher das Betriebssystem implementiert worden ist, zusätzliche Begrenzungen zur Folge haben kann, die weitaus höher sind als jene, die auf die Architektur zurückzuführen sind.

Das Wort "virtuell" in virtuellem Adressbereich steht für die gesamte Anzahl von einzigartig ansprechbaren Speicherplätzen, die einer Applikation zur Verfügung stehen, aber *nicht* für die Menge an physikalischem Speicher, der entweder im System installiert ist oder der Applikation zum jeweils gegebenen Zeitpunkt verschrieben ist.

Im Falle unserer Beispielapplikation besitzt der virtueller Adressbereich 15000 Bytes.

Um virtuellen Speicher implementieren zu können, muss das Computersystem spezielle Speicher-Management-Hardware besitzen. Diese Hardware ist auch oft als *MMU* (Memory Management Unit) bekannt. Sobald die CPU auf RAM zugreift, ändern sich ohne MMU die tatsächlichen Hauptspeicherplätze nicht — z.B. Speicheradresse 123 ist immer der selbe physikalische Speicherplatz innerhalb des Hauptspeichers (RAM).

Mit MMU durchlaufen die Speicheradressen jedoch einen Umrechnungsschritt vor jedem einzelnen Speicherzugriff. Dies bedeutet, dass Speicheradresse 123 das eine Mal zur physikalischen Adresse 82043 geleitet wird und ein anderes Mal widerum zur physikalischen Adresse 20468. Wie sich herausgestellt hat, wäre der Overhead beim individuellen Verfolgen der Umrechnungen für Billionen von Bytes viel zu hoch. Daher unterteilt MMU den Hauptspeicher in *Pages* oder auch sogennate Seiten —

Diesen Pages und deren Adress-Umrechnungen im Auge zu behalten, mag wie ein unnötiger und verwirrender Schritt klingen. Tatsächlich ist dies jedoch entscheidend bei der Implementierung virtuellen Speichers. Beachten Sie bitte dabei folgenden Punkt:

Nehmen wir unsere hypothetische Applikation mit 15000 Byte virtuellem Adressbereich und nehmen an, dass die erste Anweisung der Applikation auf Daten zugreift, die unter der Adresse 12374 gespeichert sind. Jedoch gehen wir ebenso davon aus, dass unser Computer lediglich 12288 Bytes an physikalischem Hauptspeicher besitzt. Was passiert nun, wenn die CPU versucht auf die Adresse 12374 zuzugreifen?

Was hier passiert wird als *Page Fault* oder Seitenfehler bezeichnet.

4.4.1. Seitenfehler (Page Faults)

Ein Seitenfehler oder Page Fault tritt dann auf, wenn ein Programm versucht auf Daten zuzugreifen (oder auch auf Code), welche sich zwar in deren Addressbereich, aber sich zu diesem Zeitpunkt nicht im RAM des Systems befinden. Das Betriebssystem muss Seitenfehler derart behandeln, dass irgendwie das Einlagern der Seite veranlasst wird und der Prozess nach erfolgtem Einlagern mit dem unterbrochenen Befehl fortgesetzt wird - genauso als ob der Seitenfehler niemals aufgetreten wäre.

Im Falle unserer hypothetischen Applikation legt die CPU zuerst der MMU die gewünschte Adresse (12374) vor. Jedoch besitzt die MMU keine Umwandlung für diese Adresse. Daher unterbricht diese die CPU, wobei die als "Page Fault Handler" bekannte Software ausgeführt wird. Der Page Fault Handler legt sodann genau fest, was zu tun ist, um diesen Seitenfehler zu beheben. Diese Software kann:

- Herausfinden, wo sich die gewünschte Seite auf der Festplatte befindet und diese einlesen (dies ist normalerweise der Fall, wenn es sich dabei um einen Page Fault in Bezug auf Code handelt)
- Ermitteln, dass die gewünschte Seite sich bereits im Hauptspeicher befindet (aber noch nicht dem gegenwärtigen Prozess zugewiesen ist) und die MMU rekonfigurieren, um darauf hinzuzeigen
- Hinzeigen auf eine spezielle Seite, die lediglich Nullen enthält und später dem Prozess eine neue Seite zuweisen. Dies geschieht jedoch nur unter der Voraussetzung, dass der Prozess jemals auf diese Seite schreibt (dies wird als sogenannte *Copy on Write*-Seite bezeichnet und wird oft für Seiten verwendet, die Null-initialisierte Daten enthalten).
- Holt Sie die gewünschte Seite von irgendwo anders (was später noch genauer behandelt wird)

Im Gegensatz zu den ersten drei Abläufen, die relativ unkompliziert sind, ist die Letzte nicht ganz so einfach. Dazu müssen wir einige zusätzliche Themenbereiche abdecken.

4.4.2. Die Arbeitsmenge (Working Set)

Die Menge der physikalischen Seiten, die gegenwärtig einem bestimmten Prozess gewidmet sind, werden für diesen Prozess als *Working Set* oder Arbeitsmenge bezeichnet. Die Working-Set-Größe

(Anzahl der Seiten) kann dabei wachsen und schrumpfen, abhängig von der allgemeinen Verfügbarkeit von Seiten auf einer systemweiten Basis.

Der Working Set erweitert sich, sobald ein Prozess einen Seitenfehler hervorruft. Der Working Set schrumpft, sobald immer weniger freie Seiten vorhanden sind. Um das völlige Auslaufen von Speicher zu vermeiden, müssen Seiten aus der Arbeitsmenge ausgelagert werden und in freie Seiten zur späteren Benutzung umgewandelt werden. Das Betriebssystem schrumpft Arbeitsmengen (Working Sets) von Prozessen wie folgt:

- Modifizierte Seiten werden in einen eigens dafür bestimmten Bereich auf einem Massenspeichergerät geschreiben (welcher normalerweise als *Swapping*- oder *Paging*-Space bekannt ist)
- Unmodifizierte Seiten werden als frei gekennzeichnet (es besteht kein Anlass, diese unveränderten Seiten nochmals auf eine Festplatte zu schreiben)

Um geeignete Working Sets für alle Prozesse festzulegen, muss das Betriebssystem Nutzungs-Informationen für alle Seiten ausfindig machen. Auf diese Art legt das Betriebssystem fest, welche Seiten aktiv genutzt werden (und speicher-resident bleiben) und welche Seiten nicht genutzt werden (und daher vom Speicher verdrängt werden können). In den meisten Fällen bestimmt eine Art von 'am-wenigsten-jüngst-bentutzt' Algorithmus (LRU oder auch "least recently used"), welche Seiten verdrängt werden können (da wahrscheinlich nicht mehr in einer Lokalität).

4.4.3. Seitenaustausch (Swapping)

Obwohl Swapping (das Auslagern modifizierter Seiten in den Swap-Space des Systems) ein ganz normaler Systemvorgang ist, kann auch ein Übermaß an Swapping auftreten. Warum man sich vor exzessivem Swapping hüten sollte, wird dadurch ersichtlich, dass folgende Situation immer wiederkehrend auftreten kann:

- Seiten eines Prozesses werden ausgetauscht
- Der Prozess versucht auf eine ausgetauschte Seite zuzugreifen
- Die Seite wird wieder in den Speicher eingelagert (wobei höchstwahrscheinlich die Seiten anderer Prozesse verdrängt werden)
- Kurze Zeit später wird die Seite wieder ausgelagert

Wenn die Gesamtheit der Lokalitäten aller Prozesse den Arbeitsspeicher sprengt, droht *Thrashing* oder auch Seitenflattern genannt. Dies ist ein Indikator für ungenügenden Arbeitsspeicher für die gegenwärtige Arbeitslast. Thrashing hat höchst nachteilige Auswirkungen auf das Leistungsverhalten des gesamten Systems, da eine extrem hohe CPU- und I/O-Arbeitslast durch das hektische Ein-/Auslagern generiert wird. In extremen Fällen kann es dazu kommen, dass das System tatsächlich keine nützliche Arbeit mehr leistet, da es zu beschäftigt mit dem Auslagern und Einlagern von Seiten ist.

4.5. Schlussfolgerungen zur Leistungsfähigkeit bei der Benutzung von virtuellem Speicher

Wie auch jedes andere leistungsfähige Tool hat der virtuelle Speicher, der es erlaubt umfangreichere und komplexere Applikationen einfacher zu handhaben, seinen Preis. In diesem Fall ist es die Leistungsfähigkeit — Ein OS mit virtuellem Speicher hat wesentlich mehr zu tun, als ein Betriebssystem, welches virtuellen Speicher nicht unterstützen kann. Dies bedeutet, dass das Leistungsverhalten mit virtuellem Speicher niemals so gut ist, als wenn die selbe Applikation zu 100% speicher-resident ist.

Dies ist jedoch kein Grund die Finger davon zu lassen und einfach aufzugeben. Der Nutzen, der aus virtuellem Speicher gezogen werden kann, ist einfach zu groß. Und mit ein wenig Anstrengung

kann dabei auch eine ausgezeichnete Leistungsfähigkeit erzielt werden. Dazu muss man einfach die Systemressourcen genauer betrachten, die am meisten durch die Nutzung eines virtuellen Speicher Subsystems beeinträchtigt werden.

4.5.1. Schlimmster Fall in puncto Leistungsfähigkeit

Denken wir für einen Moment über das nach, was wir in diesem Kapitel gelesen haben und betrachten genauer, welche System-Ressourcen während extrem häufigen Page Fault und Swapping Aktivitäten am meisten betroffen sind:

- RAM — Es liegt nahe, dass der verfügbare RAM niedrig ist (ansonsten würde auch kein Anlass zu Seitenfehlern oder Seitenaustausch bestehen).
- Festplatte — Während verfügbarer Speicherplatz nicht davon betroffen ist, kann dies für die I/O-Bandbreite (als Folge von häufigem Paging und Swapping) der Fall sein.
- CPU — Um die erforderlichen Prozesse, die zur Unterstützung des Speichermanagement und für I/O-Abläufe in Hinsicht auf Paging und Swapping notwendig sind durchführen zu können, wendet die CPU mehr Zyklen auf.

Die zusammenhängende Natur dieser Arbeitslaten macht es einfacher zu verstehen, wie Ressourcen-Engpässe zu ernsten Problemen im Bereich der Leistungsfähigkeit führen können.

Alles was es dazu braucht, ist offenbar ein System mit zuwenig RAM, starker Seitenfehler-Aktivität und ein System, das sich an seinen Grenzen in Bezug auf CPU oder Festplatten-I/O befindet. An diesem Punkt ist Seitenflattern (Thrashing) in Verbindung mit einer armseligen Performance unvermeidlich.

4.5.2. Bester Fall in puncto Leistungsfähigkeit

Im besten Fall stellt der dadurch erzeugte Overhead lediglich eine minimale zusätzliche Arbeitslast für ein bestens konfiguriertes System dar:

- RAM — Ausreichend RAM für alle Arbeitsmengen und gegebenenfalls auch zur Bewältigung jeglicher Seitenfehler[2]
- Festplatte — Durch die eingeschränkte Seitenfehler-Aktivität würde die I/O-Bandweite der Festplatte minimal betroffen sein.
- CPU — Die Mehrheit der CPU-Zyklen werden dazu aufgewendet, Applikationen ablaufen zu lassen und nicht den Speichermanagement-Code des Betriebssystems

Daraus ist zu ersehen, dass die Auswirkungen von virtuellem Speicher auf das allgemeine Leistungsverhalten mimimal sind, wenn dieser so wenig als möglich benutzt wird. Dies bedeutet, dass eine gute Performance von virtuellen Speicher Subsystemen auf das Vorhandensein von ausreichend RAM zurückzuführen ist.

Wichtig dabei (jedoch viel niedriger in relativer Bedeutung) sind ausreichende Festplatten-I/O- und CPU-Kapazitäten. Beachten Sie dabei, dass diese Ressourcen lediglich dabei behilflich sind, die Systemleistung bei starkem Faulting und Swapping eleganter herabzusetzen; grundsätzlich tragen diese wenig dazu bei, die Leistungsfähigkeit des virtuellen Speicher Subsystems zu unterstützen (obwohl diese offenbar eine große Rolle im Gesamt-Leistungsverhalten des Systems spielen).

2. Ein einigermaßen aktives System besitzt *immer* einen gewissen Grad an Seitenfehler-Aktivität, sobald neufreigegebene Applikationen in den Speicher gebracht werden.

4.6. Red Hat Enterprise Linux-spezifische Information

Aufgrund der Komplexität eines Betriebssystemes mit virtuellem Speicher kann die Kontrolle speicherbezogener Ressourcen unter Red Hat Enterprise Linux etwas verwirrend sein. Deshalb ist es am besten mit den einfacheren Tools zu beginnen und danach darauf aufzubauen.

Mit Hilfe des `free`-Befehls ist es möglich einen (wenn auch grob vereinfachten) Überblick über Speicher- und Swap-Nutzung zu bekommen. Hier ist ein Beispiel:

```
             total       used       free     shared    buffers     cached
Mem:       1288720     361448     927272          0      27844     187632
-/+ buffers/cache:     145972    1142748
Swap:       522104          0     522104
```

Wir stellen fest, dass dieses System 1,2GB RAM besitzt, wobei davon lediglich 350MB tatsächlich benutzt werden. Wie erwartet ist die 500MB Swap-Partion nicht in Gebrauch.

Stellen Sie das Beispiel diesem gegenüber:

```
             total       used       free     shared    buffers     cached
Mem:        255088     246604       8484          0       6492     111320
-/+ buffers/cache:     128792     126296
Swap:       530136     111308     418828
```

Das System besitzt ungefähr 256MB an RAM, wobei der Großteil benutzt wird und dadurch lediglich 8MB frei sind. Über 100MB der 512MB Swap-Partition werden benutzt. Obwohl dieses System mit Sicherheit in Hinsicht auf Speicher mehr eingeschränkt ist als das erste System, müssen wir uns doch etwas näher damit befassen, um genau feststellen zu können, ob diese Speicherlimitation Probleme hinsichtlich des Leistungsverhaltens hervorruft.

Wenn auch etwas kryptischer als `free`, besitzt der `vmstat`-Befehl den Vorteil, dass er mehr als nur Speichernutzungs-Statistiken anzeigt. Hier ist der Output des `vmstat 1 10`-Befehls:

```
   procs                  memory    swap          io     system          cpu
 r  b  w   swpd   free   buff  cache  si  so    bi    bo   in    cs  us  sy  id
 2  0  0 111304   9728   7036 107204   0   0     6    10  120    24  10   2  89
 2  0  0 111304   9728   7036 107204   0   0     0     0  526  1653  96   4   0
 1  0  0 111304   9616   7036 107204   0   0     0     0  552  2219  94   5   1
 1  0  0 111304   9616   7036 107204   0   0     0     0  624   699  98   2   0
 2  0  0 111304   9616   7052 107204   0   0     0    48  603  1466  95   5   0
 3  0  0 111304   9620   7052 107204   0   0     0     0  768   932  90   4   6
 3  0  0 111304   9440   7076 107360  92   0   244     0  820  1230  85   9   6
 2  0  0 111304   9276   7076 107368   0   0     0     0  832  1060  87   6   7
 3  0  0 111304   9624   7092 107372   0   0    16     0  813  1655  93   5   2
 2  0  2 111304   9624   7108 107372   0   0     0   972 1189  1165  68   9  23
```

Während diesem 10-sekündigen Beispiel variiert die Menge des freien Speichers ein wenig (das`free`-Feld). Ebenso wird etwas swap-bezogener I/O (das `si`- und `so`-Feld) angezeigt. Alles in allem läuft das System einwandfrei. Es ist jedoch zweifelhaft mit wieviel zusätzlicher Arbeitslast das System in Anbetracht der bereits bestehenden Speicherauslastung fertig werden könnte.

Wenn Speicher-bezogene Themen untersucht werden, ist es oft notwendig genau festzustellen, inwiefern das virtuelle Speicher Subsystem in Red Hat Enterprise Linux den Systemspeicher nutzt. Mittels dem Befehl `sar` ist es möglich, diesen Aspekt des System-Leistungsverhaltens in größerem Detail zu untersuchen.

Bei genauer Durchsicht des `sar -r`-Reports können wir Speicher- und Swap-Nutzung genauer erforschen:

```
Linux 2.4.20-1.1931.2.231.2.10.ent (pigdog.example.com)      07/22/2003

12:00:01 AM kbmemfree kbmemused  %memused kbmemshrd kbbuffers  kbcached
12:10:00 AM    240468   1048252     81.34         0    133724    485772
12:20:00 AM    240508   1048212     81.34         0    134172    485600
...
08:40:00 PM    934132    354588     27.51         0     26080    185364
Average:       324346    964374     74.83         0     96072    467559
```

Die `kbmemfree`- und `kbmemused`- Felder zeigen die typischen Statistiken zu freiem und benutztem Speicher mit dem jeweiligen Prozentsatz des benutzten Speichers an, welcher im `%memused`-Feld zu finden ist. Die `kbbuffers`- und `kbcached`-Felder zeigen an, wieviele Kilobytes Speicher den Puffern und dem systemweiten Daten-Cache zugeordnet sind.

Das `kbmemshrd`-Feld ist immer Null für Systeme (wie z.B. Red Hat Enterprise Linux), welche den 2.4 Linux Kernel benutzten.

Die Zeilen dieses Reports wurden abgeschnitten, um ihn auf dieser Seite anzeigen zu können. Hier finden Sie das, was von jeder Zeile übriggeblieben ist, mit hinzugefügter Zeitmarke auf der linken Seite, um das Lesen zu vereinfachen:

```
12:00:01 AM   kbswpfree kbswpused  %swpused
12:10:00 AM      522104         0      0.00
12:20:00 AM      522104         0      0.00
...
08:40:00 PM      522104         0      0.00
Average:         522104         0      0.00
```

In Hinsicht auf Swap-Nutzung zeigen die Felder `kbswpfree` und `kbswpused` die Menge an freiem und genutztem Swap-Space in Kilobytes an, wobei das `%swpused`-Feld den Prozentsatz an benutztem Swap-Space anzeigt.

Um mehr über Swapping-Aktivitäten zu lernen, benuzten Sie den `sar -W`-Report. Hier ist ein Beispiel:

```
Linux 2.4.20-1.1931.2.231.2.10.entsmp (raptor.example.com)      07/22/2003

12:00:01 AM  pswpin/s pswpout/s
12:10:01 AM      0.15      2.56
12:20:00 AM      0.00      0.00
...
03:30:01 PM      0.42      2.56
Average:         0.11      0.37
```

Hier beobachten wir, dass durchschnittlich dreimal sowenig Seiten von Swap hereingepaged wurden (`pswpin/s`), als umgekehrt (`pswpout/s`).

Um besser zu verstehen, wie Seiten benutzt werden, siehe dem `sar -B`-Report:

```
Linux 2.4.20-1.1931.2.231.2.10.entsmp (raptor.example.com)      07/22/2003

12:00:01 AM  pgpgin/s pgpgout/s   activepg  inadtypg  inaclnpg  inatarpg
12:10:00 AM      0.03      8.61     195393     20654     30352     49279
12:20:00 AM      0.01      7.51     195385     20655     30336     49275
...
08:40:00 PM      0.00      7.79      71236      1371      6760     15873
Average:       201.54    201.54     169367     18999     35146     44702
```

Hier können wir festlegen, wieviele Blöcke pro Sekunden von der Festplatte hereingepaged werden `pgpgin/s`) und zur Festplatte hinausgepaged werden (`pgpgout/s`). Diese Statistiken dienen als Barometer für die allgemeine Aktivität des virtuellen Speichers.

Jedoch kann mehr Wissen erlangt werden, indem die anderen Felder in diesem Report genauer geprüft werden. Der Red Hat Enterprise Linux Kernel kennzeichnet alle Seiten entweder als aktiv oder inaktiv. Wie der Name schon sagt, sind aktive Seiten auf irgendeine Art zu diesem Zeitpunkt in Verwendung (z.B. als Prozess- oder Pufferseiten), während inaktive Seiten nicht in Verwendung sind. Dieser Beispiel-Report zeigt, dass die Liste aktiver Seiten (das `activepg`-Feld) im Durchschnitt ungefähr 660MB beträgt[3].

Die restlichen Felder in diesem Report konzentrieren sich auf die inaktiveListe— Seiten, welche aus verschiedensten Gründen kürzlich nichtbenutzt worden sind. Das `inadtypg`-Feldzeigt an, wieviele inaktive Seiten *dirty*(modifiziert) sind und daher auf Festplatte geschrieben werden müssen. Das `inaclnpg`-Feld zeigt hingegen an, wieviele inaktive Seiten *clean* (unmodifiziert) sind und nicht auf die Festplatte geschrieben werden müssen.

Das `inatarpg`-Feld repräsentiert die gewünschte Größe der inaktiven Liste. Dieser Wert wird vom Linux Kernel kalkuliert und derartig festgelegt, dass die inaktive Liste groß genug bleibt, um als Pool für Seitenaustausch-Zwecke zu dienen.

Für zusätzlichen Einblick in den Seitenstatus (speziell wie oft Seiten den Status wechseln) benutzen Sie den Report `sar -R`. Hier ist ein Beispiel-Report:

```
Linux 2.4.20-1.1931.2.231.2.10.entsmp (raptor.example.com)      07/22/2003

12:00:01 AM   frmpg/s   shmpg/s   bufpg/s   campg/s
12:10:00 AM     -0.10      0.00      0.12     -0.07
12:20:00 AM      0.02      0.00      0.19     -0.07
...
08:50:01 PM     -3.19      0.00      0.46      0.81
Average:         0.01      0.00     -0.00     -0.00
```

Die Statistiken in diesem speziellen `sar`-Report sind einzigartig, was bedeutet, dass diese positiv, negativ oder null sein können. Wenn positiv, gibt der Wert die Rate an, zu der derartige Seiten zunehmen. Wenn negativ, stellt der Wert die Rate dar, zu der Seiten dieser Art abnehmen. Null bedeutet, dass die Anzahl der Seiten dieser Art weder zu- noch abnimmt.

In diesem Beispiel zeigt das letzte Sample, dass geringfügig mehr als 3 Seiten pro Sekunde von der Liste freier Seiten (das `frmpg/s`-Feld) zugeordnet wurden und beinahe 1 Seite pro Sekunde dem Page-Cache hinzugefügt worden ist (das `campg/s`-Feld). Zur Liste der als Puffer benutzten Seiten (das `bufpg/s`-Feld) ist ungefähr alle 2 Sekunden eine Seite dazugekommen, wobei die Liste von Seiten gemeinsam benutzten Speichers (das `shmpg/s`-Feld) weder Seiten dazubekommen, noch Seiten verloren hat.

4.7. Zusätzliche Ressourcen

Dieser Abschnitt beinhaltet verschiedene Ressourcen, welche dazu benutzt werden können, mehr über Ressourcenkontrolle und über das Red Hat Enterprise Linux-spezifische Thema in diesem Kapitel zu erfahren.

3. Die Seitengröße unter Red Hat Enterprise Linux auf dem x86 System beträgt in diesem konkreten Beispiel 4096 Bytes. Systeme, die auf anderen Architekturen basieren, besitzten eventuell andere Seitengrößen.

4.7.1. Installierte Dokumentation

Die folgenden Ressourcen werden im Zuge einer typischen Red Hat Enterprise Linux-Installation mitinstalliert und können Ihnen dabei behilflich sein, mehr über die in diesem Abschnitt behandelten Themen zu lernen.

- `free(1)` man-Seite — Lernen Sie Statistiken zu freiem und benutztem Speicher anzuzeigen.
- `vmstat(8)` man-Seite — Lernen Sie einen präzisen Überblick über Prozess-, Speicher-, Swap-, I/O-, System- und CPU-Nutzung zu erstellen.
- `sar(1)` man-Seite — Lernen Sie Reporte über die Systemressourcen-Nutzung zu erstellen.
- `sa2(8)` man-Seite — Lernen Sie Dateien zu den Reporten über die tägliche Systemressourcen-Nutzung zu erstellen.

4.7.2. Nützliche Webseiten

- http://people.redhat.com/alikins/system_tuning.html — System-Tuning-Info für Linux Server. Eher unkonventionelle Methoden zum Thema Performance-Tuning und Ressourcenkontrolle für Server.
- http://www.linuxjournal.com/article.php?sid=2396 — Tools zur Performance-Kontrolle für Linux. Diese Linux Journalseite ist mehr in Richtung Administrator ausgelegt, der darin interessiert ist, eine maßgeschneiderte Lösung zur Darstellung eines Leistungsdiagrammes zu schreiben. Bereits vor einigen Jahren geschrieben, kann es durchaus sein, dass einige Details nicht mehr länger zutreffend sind. Das Gesamtkonzept und die Ausführung hingegen sind einwandfrei.

4.7.3. Bücher zum Thema

Die folgenden Bücher behandeln verschiedenste Themen in Bezug auf Ressourcenkontrolle und sind gute Nachschlagewerke für Red Hat Enterprise Linux-Systemadministratoren:

- *Red Hat Enterprise Linux Handbuch zur System-Administration*; Red Hat, Inc. — beinhaltet ein Kapitel über einige der Überwachungstools, die hier behandelt wurden.
- *Linux Performance Tuning and Capacity Planning* von Jason R. Fink und Matthew D. Sherer; Sams — Gibt einen detailgenaueren Überblick über die bereits vorgestellten Tools zur Ressourcenkontrolle und beinhaltet auch andere Tools, die sich bestens für spezifischere Ressourcenkontroll-Bedürfnisse eignen.
- *Red Hat Linux Security and Optimization* von Mohammed J. Kabir; Red Hat Press — Die ersten ungefähr 150 Seiten dieses Buches behandeln leistungsbezogene Themen. Dies beinhaltet Kapitel, die Leistungsfragen in Bezug auf Netzwerk, Internet, e-Mail und Dateiserver behandeln.
- *Linux Administration Handbook* von Evi Nemeth, Garth Snyder und Trent R. Hein; Prentice Hall — Stellt ein kurzes Kapitel zur Verfügung, welches sich in einem ähnlichen Rahmen wie dieses Buch befindet, mit der Ausnahme eines interessanten Abschnittes über die Diagnose eines Systems, das plötzlich langsamer geworden ist.
- *Linux System Administration: A User's Guide* von Marcel Gagne; Addison Wesley Professional — Beinhaltet ein kurzers Kapitel über Leistungskontrolle und Tuning.
- *Essential System Administration* (3. Ausgabe) von Aeleen Frisch; O'Reilly & Associates — Das Kapitel über die Verwaltung von System-Ressourcen beinhaltet gute Allgemeininformationen mit einigen Linux-spezfischen Beiträgen.
- *System Performance Tuning* (2. Ausgabe) von Gian-Paolo D. Musumeci und Mike Loukides; O'Reilly & Associates — Obwohl eine starke Tendenz zu mehr traditionellen

UNIX-Implementationen besteht, gibt es auch viele Linux-spezifische Referenzen durch das ganze Buch hindurch.

Kapitel 5.

Speicher verwalten

Wenn es etwas gibt, das die meiste Arbeitszeit eines Systemadministrators in Anspruch nimmt, dan ist es die Speicherverwaltung. Es scheint, dass Festplatten immer zu wenig freien Speicherplatz haben, immer mit zu viel I/O-Aktivitäten überladen werden oder unerwartet ausfallen. Es ist daher notwendig, über ein solides Wissen über Festplattenspeicher zu verfügen, um ein erfolgreicher Systemadministrator zu sein.

5.1. Ein Überblick über Speicher-Hardware

Bevor Sie Speicher verwalten, müssen Sie als erstes die Hardware verstehen, auf der Daten gespeichert werden. Sie sollten zumindest ein Grundverständnis über Massenspeicher haben, ansonsten stehen Sie vielleicht irgendwann vor einem Speicher-bezogenen Problem, aber haben nicht das Hintergrundwissen, um das was Sie sehen richtig zu interpretieren. Indem Sie Einsichten in den Hardwarebetrieb gewinnen, sind Sie in der Lage entscheiden zu können, ob das Speicher-Subsystem Ihres Computers ordnungsgemäß funktioniert.

Der größte Teil der Massenspeichergeräte verwendet gewisse rotierende Medien und unterstützt den willkürlichen Zugriff auf Daten auf diesen Medien. Dies bedeutet, dass folgende Komponenten in fast jedem Speichergerät zu finden sind:

- Disk Platten
- Daten Schreib-/Lesegerät
- Zugriffsarme

In den folgenden Abschnitten werden diese Komponenten im Detail beschrieben.

5.1.1. Disk Platten

Das rotierende Medium, das von fast allen Massenspeichergeräten verwendet wird, besteht aus einer oder mehreren flachen, kreisförmigen Platten. Die Platte kann aus einer Vielzahl verschiedener Materialien, wie zum Beispiel Aluminium, Glas oder Polycarbonat bestehen.

Die Oberfläche jeder Platte wird speziell für das Speichern von Daten bearbeitet. Die genaue Behandlung hängt von der Art der zu verwendenden Datenspeichertechnologie ab. Die am häufigsten eingesetzte Methode basiert auf Magnetismus; in diesen Fällen sind die Platten mit einem Mischpräparat beschichtet, welches gute magnetische Charakteristiken aufweist.

Eine weitere häufige Methode der Speichertechnologie basiert auf optischen Prinzipien. In diesem Fall sind die Platten mit Materialien beschichtet, deren optische Eigenschaften geändert werden können, sodass Daten hierauf optisch[1] gespeichert werden können.

Egal welche Technologie benutzt wird, es werden bei allen diesen Speichertechnologien die PLatten gedreht, was der gesamten Oberfläche erlaubt, an einer anderen Komponente vorbeizustreichen — dem Daten-Lese/Schreib-Gerät.

1. Einige optische Geräte — insbesondere CD-ROM-Laufwerke — verwenden andere Methoden zur Datenspeicherung; diese Unterschiede werden an den entsprechenden Stellen in diesem Kapitel behandelt.

5.1.2. Daten Schreib-/Lesegerät

Das Daten-Lese/Schreib-Gerät ist die Komponente, welche die Bits und Bytes eines Computersystems in optische oder magnetische Variationen umwandelt, die zur Kommunikation mit den Materialien, welche zur Beschichtung der Platten verwendet worden sind, notwendig sind.

Manchmal sind die Bedingungen, unter denen diese Geräte arbeiten müssen, geradezu eine Herausforderung. So müssen zum Beispiel für magnetische Speichergeräte die Lese-/Schreib-Geräte (auch als *Köpfe* bezeichnet) sich in sehr geringem Abstand zur Oberfläche der Platte befinden. Wenn sich jedoch Köpfe und Platte berühren, würde die daraus resultierende Reibung schweren Schaden an Kopf und Platte anrichten. Aus diesem Grund sind die Oberflächen von Köpfen und Platten sorgfältig poliert und die Köpfe verwenden den von der sich drehenden Platte entstehenden Luftdruck, um über der Plattenoberfläche zu "schweben"; in einer Höhe, die geringer ist als die Dicke eines menschlichen Haares. Deswegen sind magnetische Festplatten so anfällig für Erschütterungen, plötzliche Temperaturänderungen und jegliche durch Luft übertragene Verschmutzung.

Die Probleme, die bei optischen Köpfen auftauchen können, unterscheiden sich von denen für magnetische Köpfe — hier müssen die Köpfe sich in einem relativ konstanten Abstand zur Oberfläche der Platte befinden. Ansonsten können die Linsen, die auf die Platte gerichtet sind, kein ausreichend scharfes Bild produzieren.

In beiden Fällen verwenden die Köpfe jedoch nur einen Bruchteil der Plattennoberfläche für das Speichern der Daten. Indem sich die Platte unter den Köpfen dreht, nimmt dieser Teil der Oberfläche die Form einer sehr dünnen kreisförmigen Linie an.

Dies würde jedoch bedeuten, dass mehr als 99% der Plattenoberfläche verschwendet würden. Man könnte zusätzliche Köpfe über der Platte installieren, um die Oberfläche voll auszunutzen, wobei hierfür mehr als tausend Köpfe eingesetzt werden müssten, um die gesamte Oberfläche abzudecken. Was benötigt wird, ist eine Methode, mit der die Köpfe über die gesamte Oberfläche der Platte bewegt werden können.

5.1.3. Zugriffsarme

Indem man den Kopf an einem Arm befestigt, der über die gesamte Oberfläche der Platte schwebt, ist es möglich, diese in vollem Umfang für die Datenspeicherung zu verwenden. Der Zugriffsarm muss jedoch zwei Dinge können:

- Sich sehr schnelle bewegen
- Sich sehr genau bewegen

Der Zugriffsarm muss sich so schnell wie möglich bewegen können, da jegliche Zeit, die zum Bewegen des Arms von einer Position zur nächsten benötigt wird, verschwendete Zeit ist. Dies liegt daran, dass keine Daten geschrieben werden können, solange sich der Arm noch in Bewegung befindet[2].

Der Zugriffsarm muss sich mit großer Präzision bewegen, da wie bereits erwähnt die vom Kopf abgetastete Oberfläche sehr klein ist. Aus diesem Grund wird zur effizienten Nutzung der Speicherkapazität der Kopf gerade nur soweit bewegt, dass sichergestellt wird, dass Daten in der neuen Position keine Daten überschreiben, die in der vorhergehenden Position geschrieben worden sind. Hieraus resultiert der Effekt der Aufteilung der Plattenoberfläche in tausende, konzentrische "Ringe" oder *Tracks*. Die Bewegung des Zugriffsarms von einem Track zum nächsten wird häufig als *Seeking* bezeichnet und die hierfür benötigte Zeit als *Seek-Time* oder Suchzeit.

2. Bei einigen optischen Geräten (wie CD-ROM-Laufwerke) ist der Arm ständig in Bewegung und erzeugt so eine spiralförmige Linie des Kopfes auf der Platte. Dies ist ein grundlegender Unterschied in der Verwendung des Speichermediums und reflektiert die Herkunft der CD-ROM aus dem Musikbereich, wo kontinuierliches Abrufen von Daten häufiger benötigt wird als das punktgenaue Suchen.

Gibt es mehrere Platten (oder eine Platte, bei der beide Seiten für die Datenspeicherung verwendet werden), sind die Arme für jede Oberfläche übereinander "gestapelt" angebracht; es kann also simultan auf den selben Track auf jeder Oberfläche zugegriffen werden. Könnten die Tracks für jede Oberfläche bildlich dargestellt werden, mit dem Zugriff statisch über einem Track, so würden diese übereinander gestapelt in der Form eines Zylinders erscheinen. Aus diesem Grund werden die Tracks, auf die an einer bestimmten Position der Zugriffsarme zugegriffen werden kann, als *Zylinder* bezeichnet.

5.2. Konzepte der Speicheradressierung

Die Konfiguration von Platten, Köpfen und Zugriffsarmen macht es möglich, den Kopf über jedem Teil jeder Oberfläche jeglicher Platte im Speichergerät zu positionieren. Dies reicht jedoch nicht aus, um die Speicherkapazität voll auszunutzen. Es bedarf daher einer Methode, bei der Adressen an einheitlich große Teile des verfügbaren Speichers vergeben werden können.

Hierbei ist noch einen letzter Aspekt in diesem Prozess zu beachten. Berücksichtigen Sie alle Tracks in den vielen Zylindern eines herkömmlichen Massenspeichergerätes. Da die Tracks verschiedene Durchmesser haben, variiert auch deren Umfang. Wenn daher Speicher nur auf den Tracklevel adressiert werden würde, so würde jeder Track eine andere Menge an Daten besitzen — Track #0 (nahe dem Mittelpunkt der Platte) würde z.B. 10 827 Bytes enthalten während Track #1 258 (nahe der Außenkante der Platte) 15 382 Bytes enthalten würde.

Die Lösung ist, die Tracks in mehrere *Sektoren* oder *Blöcke* von gleichgroßen (meistens 512 Bytes) Speichersegmenten zu unterteilen. Das Ergebnis ist eine feste Anzahl von Sektoren pro Track[3].

Ein Nebeneffekt dabei ist, dass jeder Track ungenutzten Speicherplatz enthält — nämlich den Platz zwischen den Sektoren. Trotz der konstanten Anzahl der Sektoren pro Track unterscheidet sich die Größe des ungenutzten Speicherplatzes — relativ wenig ungenutzter Speicherplatz in den inneren Tracks und sehr viel mehr in den äußeren Tracks. In jedem Fall ist ungenutzter Platz eine Verschwendung, da allfällige Daten hierauf nicht gespeichert werden können.

Der Vorteil der Versetzung dieses ansonsten verschwendeten Speicherplatzes ist jedoch, dass die effektive Adressierung des Speichers auf einem Massenspeichergerät möglich ist. Es gibt zwei Methoden für die Adressierung — Geometrie-basierte Adressierung und Block-basierte Adressierung.

5.2.1. Geometrie-basierte Adressierung

Der Begriff *Geometrie-basierte Adressierung* bezieht sich auf die Tatsache, dass Massenspeichergeräte Daten an einem bestimmten physikalischen Ort auf dem Speichermedium speichern. Im Falle der hier beschriebenen Geräte bezieht sich dies auf drei spezielle Dinge, die einen bestimmten Punkt auf der Platte des Geräts definieren:

- Zylinder
- Kopf
- Sektor

Die folgenden Abschnitte behandeln wie eine hypothetische Adresse einen bestimmten physikalischen Ort auf dem Speichermedium beschreiben kann.

3. Während frühere Massenspeichergeräte die gleiche Anzahl von Sektoren für jeden Track verwendeten, teilen neuere Geräte die Zylinder in verschiedene "Zonen" auf, bei denen jede Zone eine unterschiedliche Anzahl von Sektoren pro Track hat. Der Grund hierfür ist das Ausnutzen des zusätzlichen Speicherplatzes zwischen den Sektoren in den äußeren Zylindern, bei denen mehr ungenutzter Speicherplatz zwischen den Sektoren vorhanden ist.

5.2.1.1. Zylinder

Wie bereits erwähnt, bezeichnet der Zylinder eine bestimmte Position des Zugriffsarms (und dadurch der Lese/Schreib-Köpfe). In dem wir einen bestimmten Zylinder angeben, eliminieren wir alle anderen Zylinder und reduzieren somit die Suche auf einen einzigen Track für jede Oberfläche im Massenspeichergerät.

Zylinder	Kopf	Sektor
1014	*X*	*X*

Tabelle 5-1. Speicher-Adressierung

Unter Tabelle 5-1 wurde der erste Teil einer Geometrie-basierten Adresse bereits ausgefüllt. Die beiden anderen Komponenten dieser Adresse — Kopf und Sektor — bleiben unspezifiziert.

5.2.1.2. Kopf

Auch wenn wir genaugenommen eine bestimmte Platte auswählen, da jede Oberfläche einen Lese/Schreib-Kopf zugewiesen hat, ist es einfacher, dies als Interaktion mit einem bestimmten Kopf zu betrachten. Die Elektronik des Gerätes wählt in der Tat einen Kopf aus und — da alle anderen nicht ausgewählt sind — interagiert nur mit dem ausgewählten Kopf für die Dauer des I/O-Betriebes. Alle anderen Tracks, aus denen der aktuelle Zylinder besteht, wurden nunmehr eliminiert.

Zylinder	Kopf	Sektor
1014	2	*X*

Tabelle 5-2. Speicher-Adressierung

Unter Tabelle 5-2 wurden die ersten beide Teile einer Geometrie-basierten Adresse bereits ausgefüllt. Eine letzte Komponente dieser Adresse — der Sektor — ist noch unbestimmt.

5.2.1.3. Sektor

Indem wir einen bestimmten Sektor angeben, ist die Adressierung vollständig und hat den gewünschten Datenblock eindeutig identifiziert.

Zylinder	Kopf	Sektor
1014	2	12

Tabelle 5-3. Speicher-Adressierung

Unter Tabelle 5-3 wurde die vollständige Geometrie-basierte Adresse bereits ausgefüllt. Diese Adresse identifiziert den Ort eines bestimmten Blockes unter allen anderen Blöcken auf diesem Gerät.

5.2.1.4. Probleme bei Geometrie-basierter Adressierung

Während Geometrie-basierte Adressierung relativ unkompliziert ist, gibt es einen mehrdeutigen Bereich, der problematisch werden kann. Die Doppeldeutigkeit liegt in der Nummerierung von Zylindern, Köpfen und Sektoren.

Es ist wahr, dass jede Geometrie-basierte Adresse einen bestimmten Datenblock eindeutig identifiziert; dies gilt jedoch nur, wenn die Nummerierung von Zylindern, Köpfen und Sektoren nicht geändert wird. Ändert sich die Nummerierung (wenn sich zum Beispiel die Hardware/Software für das Speichergerät ändert), ändert sich somit auch das Mapping zwischen Geometrie-basierten Adressen und den zugehörigen Datenblöcken, was ein Zugreifen auf die gewünschten Daten unmöglich macht.

Aufgrund dieser möglichen Mehrdeutigkeit wurde ein anderer Ansatz für die Adressierung entwickelt. Der nächste Abschnitt beschreibt dies eingehender.

5.2.2. Block-basierte Adressierung

Block-basierte Adressierung ist wesentlich unkomplizierter als Geometrie-basierte Adressierung. Bei der Block-basierten Adressierung wird jedem Block eine einzigartige Nummer gegeben. Diese Nummer wird vom Computer zum Massenspeichermedium weitergeleitet, welches dann intern die Umwandlung in eine Geometrie-basierte Adresse, die vom Schaltkreis des Geräts benötigt wird, durchführt.

Da die Umwandlung in eine Geometrie-basierte Adresse immer vom Gerät selbst durchgeführt wird, ist diese auch immer konsistent und eliminiert somit das Problem, das der Vergabe von Geometrie-basierten Adressen inhärent ist.

5.3. Schnittstellen der Massenspeichergeräte

Jedes Gerät, das in einem Computersystem verwendet wird, muss auf irgendeine Art mit diesem verbunden sein. Dieser Anschlusspunkt wird als *Schnittstelle* oder Interface bezeichnet. Massenspeichergeräte machen hier keinen Unterschied — auch diese haben Schnittstellen. Schnittstellen sind aus zwei Gründen wichtig:

- Es gibt viele verschiedene (größtenteils inkompatible) Schnittstellen
- Verschiedene Schnittstellen unterscheiden sich durch unterschiedliche Performance und Preismerkmale

Leider gibt es keine universelle Geräteschnittstelle und noch nicht einmal eine einzige Schnittstelle für Massenspeichergeräte. Aus diesem Grund müssen Administratoren auf die von den Unternehmensystemen unterstützten Schnittstellen achten. Ansonsten besteht das Risiko, dass die falsche Hardware bei einem Systemupgrade angeschafft wird.

Verschiedene Schnittstellen haben verschiedene Performance-Kapazitäten, die einige Schnittstellen geeigneter für bestimmte Umgebungen machen als andere. So sind zum Beispiel Schnittstellen, die Hochgeschwindigkeitsgeräte unterstützen können, besser für Serverumgebungen geeignet, während langsamere Schnittstellen für die Desktop-Verwendung ausreichen. Unterschiede in der Leistung führen unausweichlich auch zu Unterschieden im Preis, was — wie immer — bedeutet, dass Sie das bekommen, wofür Sie bezahlen. Hochleistungs-Computing hat seinen Preis.

5.3.1. Historischer Hintergrund

Über die Jahre hinweg wurden viele verschiedene Schnittstellen für Massenspeichergeräte entwickelt. Einige blieben auf der Strecke, andere werden heute noch verwendet. Die folgende Liste bietet einen Überblick über das Ausmaß der Schnittstellenentwicklung in den letzten 30 Jahren und eine Perspektive für die Schnittstellen, die heutzutage verwendet werden.

FD-400

Eine Schnittstelle, die ursprünglich für die damaligen 8" Floppy-Diskettenlaufwerke Mitte der 70er Jahre entwickelt wurde. Ein 44-Pin-Kabel und einem Schaltkreis-Steckverbinder, der Strom und Daten lieferte, wurde dabei verwendet.

SA-400

Eine andere Floppy-Diskettenschnittstelle (diesmal ursprünglich Ende der 70er Jahre für die damals neuen 5.25" Floppy-Laufwerke entwickelt). Verwendete ein 34-Pin-Kabel mit einem Standard Steckverbinder. Eine leicht abgeänderte Version dieser Schnittstelle wird heute noch für 5.25" Floppy- und 3.5" Diskettenlaufwerke verwendet.

IPI

Steht für Intelligentes Peripherie Interface. Diese Schnittstelle wurde auf 8 und 14-inch Festplatten für Minicomputer der 70er Jahre verwendet.

SMD

Als Nachfolger von IPI wurde SMD (Storage Module Device) auf 8- und 14-inch Minicomputer-Festplatten in den 70er und 80er Jahren verwendet.

ST506/412

Eine Festplattenschnittstelle der frühen 80er Jahre. Wurde in vielen PCs eingesetzt und verwendet 2 Stecker — einen mit 34 Pins, und einen mit 20 Pins.

ESDI

Steht für Enhanced Small Device Interface. Diese Schnittstelle wurde als Nachfolger zur ST506/412 mit schnelleren Transferraten und größeren unterstützten Laufwerksgrößen betrachtet. Ab Mitte der 80er Jahre verwendet, benutzt ESDI das gleiche zwei-Kabel-Schema wie sein Vorgänger.

Es gab damals auch proprietäre Schnittstellen von größeren Computerherstellern (hauptsächlich IBM und DEC). Die Absicht hinter der Entwicklung dieser Schnittstellen war der Versuch, das extrem lukrative Peripherie-Geschäft für deren Computer zu sichern. Durch die proprietäre Natur waren die Geräte, die mit diesen Schnittstellen kompatibel waren, jedoch wesentlich teurer als vergleichbare nicht-proprietäre Geräte. Aus diesem Grund erreichten diese Schnittstellen niemals eine langfristige Beliebtheit.

Während proprietäre Schnittstellen weitestgehend verschwunden sind und die hier beschriebenen Schnittstellen kaum noch Marktanteile besitzen, ist es doch wichtig, über diese nicht mehr länger benutzten Schnittstellen Bescheid zu wissen, da dies zumindest eines deutlich werden lässt — nichts in der Computerindustrie bleibt lange konsistent. Halten Sie also ständig Ausschau nach neuen Schnittstellen-Technologien; eines Tages werden Sie vielleicht eine finden, die besser für Ihre Anforderungen geeignet ist, als jene, die Sie bisher verwendet haben.

5.3.2. Heutige Industrie-Standard-Schnittstellen

Im Gegensatz zu den proprietären Schnittstellen, die im vorherigen Abschnitt beschrieben wurden, wurden einige weitestgehend angenommen und zum Industrie-Standard gewählt. Insbesondere zwei Schnittstellen haben diesen Übergang geschafft und sind ein bedeutendes Kernstück in der heutigen Speicherindustrie:

- IDE/ATA
- SCSI

5.3.2.1. IDE/ATA

IDE steht für Integrated Drive Electronics. Diese Schnittstelle stammt aus den späten 80er Jahren und verwendet 40-Stift Stecker.

Anmerkung

Der eigentliche Name für diese Schnittstelle ist "AT-Attachment" (oder ATA), der Begriff "IDE" (der sich eigentlich auf ein ATA-kompatibles Massenspeichergerät bezieht) wird jedoch weitläufig verwendet. Im restlichen Teil dieses Abschnitts verwenden wir jedoch den richtigen Namen der Schnittstelle — ATA.

ATA implementiert eine Bus-Topologie, bei der jeder Bus zwei Massenspeichergeräte unterstützt. Diese beiden Geräte werden als *Master* und *Slave* bezeichnet. Diese Begriffe sind irreführend, da eine Art Beziehung zwischen diesen Geräten impliziert wird; dies ist jedoch nicht der Fall. Die Auswahl, welches Gerät der Master und welches der Slave ist, wird gewöhnlich durch die Jumper-Blöcke in jedem Gerät festgelegt.

Anmerkung

Eine neuere Innovation ist die Einführung von *Cable-Select*-Fähigkeiten für ATA. Diese Innovation erfordert die Verwendung eines bestimmten Kabels, einem ATA-Controller und einem Massenspeichergerät, das Cable-Select (normalerweise durch eine "Cable-Select" Jumper-Einstellung) unterstützt. Ist dies richtig konfiguriert, eliminiert Cable-Select die Notwendigkeit, Jumper beim Umstellen von Geräten auszuwechseln; anstelle dessen legt die Geräte-Position am ATA-Kabel fest, ob dieses Master oder Slave ist.

Eine Variation dieser Schnittstelle illustriert die einzigartigen Methoden, mit denen Technologien vermischt werden können und führt desweiteren unsere nächste Industrie-Standard-Schnittstelle ein. *ATAPI* ist eine Variation der ATA-Schnittstelle und steht für AT Attachment Packet Interface. Hauptsächlich von CD-ROM-Laufwerken verwendet, hält sich ATAPI an die elektrischen und mechanischen Aspekte der ATA-Schnittstelle, verwendet jedoch das Kommunikationsprotokoll der im nächsten Abschnitt beschriebenen Schnittstelle — SCSI.

5.3.2.2. SCSI

Formell als Small Computer System Interface bekannt stammt SCSI aus den frühen 80er Jahren und wurde im Jahre 1986 zum Standard. Wie auch ATA verwendet SCSI eine Bus-Topologie. Hier endet jedoch auch schon die Ähnlichkeit.

Die Verwendung einer Bus-Topologie bedeutet, dass jedes Gerät auf dem Bus irgendwie eindeutig identifiziert werden muss. Während ATA nur zwei verschiedene Geräte für jeden Bus unterstützt und diesen einen eindeutigen Namen zuweist, tut SCSI dies, indem jedem Gerät auf dem SCSI-Bus eine eindeutige numerische Adresse oder *SCSI-ID* zugewiesen wird. Jedes Gerät auf einem SCSI-Bus muss dahingehend konfiguriert werden (meistens durch Jumper oder Switches[4]), auf die SCSI-ID zu antworten.

Bevor wir fortfahren, ist es wichtig zu erwähnen, dass der SCSI-Standard nicht eine einzige Schnittstelle beschreibt, sondern eine Familie von Schnittstellen. SCSI variieren in mehreren Bereichen:

4. Einige Speicher-Hardware (meistens solche, die austauschbare Laufwerkträger haben) wurde so entwickelt, dass das Einstecken eines Moduls die SCSI-ID automatisch auf den richtigen Wert setzt.

- Busbreite
- Busgeschwindigkeit
- Elektrische Merkmale

Der ursprüngliche SCSI-Standard beschrieb eine Bus-Topologie, in der acht Leitungen im Bus für den Datentransfer verwendet wurden. Dies bedeutete, dass das erste SCSI-Gerät nur 1 Byte Daten auf einmal übertragen konnte. Zu einem späteren Zeitpunkt wurde der Standard auf Implementierungen mit 16 Leitungen ausgeweitet, was die zu übertragende Datenmenge verdoppelte. Die eigentliche "8-Bit" SCSI-Implementierung wurde sodann als *narrow* SCSI bezeichnet, während die neuere 16-Bit-Implementierung als *wide* SCSI bekannt wurde.

Ursprünglich wurde die Busgeschwindigkeit für SCSI auf 5 MHz gesetzt, was eine Transferrate von 5MB/Sekunde auf einem 8-Bit SCSI-Bus erlaubte. Erweiterungen des Standards verdoppelten diese Geschwindigkeit auf 10 MHz, d.h. 10MB/Sekunde für narrow SCSI und 20 MB/Sekunde für wide SCSI. Wie bei der Busbreite erhielten die Änderungen in der Busgeschwindigkeit neue Namen, die 10 MHz Busgeschwindigkeit wurde als *fast* bezeichnet. Spätere Erweiterungen brachten die Busgeschwindigkeiten auf *ultra* (20MHz), *fast-40* (40MHz) und *fast-80*[5]. Weitere Erhöhungen der Transferraten führten zu mehreren unterschiedlichen Versionen der *ultra160* Busgeschwindigkeit.

Durch eine Kombination dieser Begriffe können unterschiedliche SCSI-Konfigurationen genau benannt werden. So ist zum Beispiel eine "ultra-wide" SCSI ein 16-bit SCSI-Bus bei 20 MHz.

Der ursprüngliche SCSI-Standard verwendete *Einzelsignale*. Dies ist eine elektrische Konfiguration, bei der nur ein Leiter ein elektrisches Signal weitergibt. Später kamen dann *Differentialsignale* hinzu, bei denen zwei Leiter für das Weiterleiten von elektrischen Signalen eingesetzt wurden. Differential-SCSI (was später in *Hochspannungsdifferential* oder HVD SCSI umbenannt wurde) hat den Vorteil verringerter Empfindlichkeit auf elektrisches Rauschen und ermöglichte längere Kabellängen; hat sich jedoch nie im allgemeinen Computermarkt durchgesetzt. Eine spätere Implementation, die als *Niederspannungsdifferential* (LVD/Low Voltage Differential) bekannt wurde, hat sich letztendlich durchgesetzt und ist eine Voraussetzung für höhere Busgeschwindigkeiten.

Die Breite eines SCSI-Busses bestimmt nicht nur die Datenmenge, die mit jedem Clock-Zyklus übertragen werden kann, sondern auch wieviele Geräte an einen Bus angeschlossen werden können. Herkömmliche SCSI unterstützen 8 einzigartig adressierte Geräte, während von wide SCSI 16 unterstützt werdeb. In jedem Fall müssen Sie sicherstellen, dass alle Geräte eine jeweils einzigartige SCSI-ID verwenden. Haben zwei Geräte die gleiche ID, bringt dies Probleme mit sich, die zu Datenkorruption führen können.

Darüberhinaus sollten Sie beachten, dass *jedes* Gerät auf dem Bus eine ID verwendet. *Dies umfasst auch den SCSI-Controller.* Häufig wird dies von Administratoren vergessen und setzen versehentlich die selbe SCSI-ID für ein Gerät sowie auch für den SCSI-Controller. Dies bedeutet in der Praxis, dass nur 7 (oder 15) Geräte auf einem Bus zur Verfügung stehen, da jeder Bus eine ID für den Controller bereitstellen muss.

Tipp

Die meisten SCSI-Implementierungen enthalten eine Methode zum Scannen des SCSI-Busses; dies wird häufig dazu verwendet, zu bestätigen, dass alle Geräte ordnungsgemäß konfiguriert sind. Ist das Ergebnis des Bus-Scans das gleiche Gerät für jede einzelne SCSI-ID, so wurde dieses Gerät fälschlicherweise auf die gleiche SCSI-ID wie der SCSI-Controller gesetzt. Um dieses Problem zu lösen, müssen Sie das Gerät auf eine andere (und einzigartige) SCSI-ID umkonfigurieren.

5. Fast-80 ist technisch gesehen keine Änderung der Busgeschwindigkeit, da der 40MHz Bus erhalten wurde; die Daten wurden jedoch beim Steigen und Fallen jedes Clock-Impulses gesendet, was den Durchsatz effektiv verdoppelt.

Aufgrund der bus-orientierten Architektur ist es nötig, beide Enden des Busses richtig *abzuschließen*. Für diesen Abschluss wird ein terminierter Stecker mit dem richtigen elektrischen Widerstand an jeden Leiter des SCSI-Busses angebracht. Endwiderstände sind eine elektrische Voraussetzung. Ohne diese würden die vielen Signale auf dem Bus von den Enden des Busses reflektiert und somit die gesamte Kommunikation beeinträchtigt werden.

Viele (jedoch nicht alle) SCSI-Geräte haben interne Endwiderstände, die mittels Jumpern oder Switches aktiviert oder deaktiviert werden können. Externe Endwiderstände sind außerdem erhältlich.

Eines sollten Sie jedoch über SCSI im Hinterkopf behalten — es ist nicht nur ein Schnittstellen-Standard für Massenspeichergeräte. Viele andere Geräte (wie Scanner, Drucker und Kommunikationsgeräte) verwenden SCSI, auch wenn diese weniger oft vorkommen als SCSI-Massenspeichergeräte. Jedoch mit dem Aufkommen von USB und IEEE-1394 (auch Firewire genannt) werden diese Schnittstellen in Zukunft häufiger für solche Geräte eingesetzt werden.

Tipp

Die USB- und IEEE-1394-Schnittstellen bewegen sich auch langsam in Richtung Massenspeichergeräte, es gibt zur Zeit jedoch noch keine nativen USB- oder IEEE-1394-Massenspeichergeräte auf dem Markt. Anstelle dessen werden heutzutage ATA- oder SCSI-Geräte mit externen Umwandlungsschaltkreisen angeboten.

Egal welche Schnittstelle ein Massenspeichergerät verwendet, das Innenleben dieser Geräte hat einen Einfluss auf dessen Performance. Im folgenden Abschnitt wird dieses wichtige Thema behandelt.

5.4. Performance-Merkmale der Festplatte

Die Performance-Besonderheiten der Festplatte wurden bereits im Kapitel Abschnitt 4.2.4 angeschnitten; dieser Abschnitt beschreibt das Thema jetzt tiefergehend. Es ist wichtig für Systemadministratoren zu verstehen, dass ohne zumindest grundlegende Kenntnisse über die Funktionsweise von Festplatten es sogar möglich ist, dass unwissentlich Änderungen an der Systemkonfiguration vorgenommen werden, welche wiederum die gesamte Perfomance negativ beeinflussen könnten.

Die Zeit, die eine Festplatte benötigt eine I/O-Anfrage zu beantworten und abzuschließen, hängt von zwei Dingen ab:

- Mechanische und elektrische Einschränkungen der Festplatte
- I/O-Last des Systems

In den folgenden Abschnitten werden die Aspekte der Festplatten-Performance tiefergehend beschrieben.

5.4.1. Mechanische/Elektrische Einschränkungen

Da Festplatten elektro-mechanische Geräte sind, unterliegen diese bestimmten Einschränkungen in Bezug auf Geschwindigkeit und Performance. Jede I/O-Anfrage erfordert, dass die verschiedenen Komponenten der Festplatte zusammenarbeiten, um diese Anfrage bearbeiten zu können. Da alle diese Komponenten verschiedene Leistungsmerkmale haben, wird die Gesamtleistung der Festplatte durch die Summe der Leistungen der einzelnen Komponenten bestimmt.

Die elektronischen Komponenten sind wesentlich schneller als die Mechanischen. Aus diesem Grund haben die mechanischen Komponenten den größten Einfluss auf die Performance der Festplatte.

Tipp

Der effektivste Weg, die Performance der Festplatte zu verbessern, ist die mechanische Aktivität der Festplatte soweit wie möglich zu reduzieren.

Die durchschnittliche Zugriffszeit einer typischen Festplatte ist rund 8.5 Millisekunden. In den folgenden Abschnitten wird diese Zahl in größerem Detail dargestellt und gezeigt, wie jede Komponente die Gesamt-Performance der Festplatte beeinflussen kann.

5.4.1.1. Befehlsverarbeitungszeit

Alle modernen Festplatten haben hochentwickelte, eingebettete Computersysteme, die deren Betrieb steuern. Diese Computersysteme führen folgende Aufgaben aus:

- Interaktion mit der Außenwelt durch die Schnittstelle der Festplatte
- Steuern des Betriebs der restlichen Hardware über die Komponenten der Festplatte, Erholen von jeglichen Fehlerzuständen, die eventuell aufgetreten sind
- Verarbeitung der Ursprungsdaten, die vom eigentlichen Speichermedium gelesen und auf dieses geschrieben werden

Auch wenn in Festplatten verwendetee Mikroprozessoren relativ leistungsstark sind, benötigen die ihnen zugewiesenen Aufgaben Zeit zur Bearbeitung. Durchschnittlich liegt diese Zeit bei etwa 0,003 Millisekunden.

5.4.1.2. Lese-/Schreib-Köpfe

Die Lese-/Schreib-Köpfe der Festplatte funktionieren nur, wenn die Festplatten, über denen sie "fliegen", sich drehen. Da Daten durch die Bewegung der Medien unter den Köpfen geschrieben oder gelesen werden, ist die Zeit, die von den Medien, welche die gewünschten Sektoren enthalten, benötigt wird um unter dem Kopf vorbeizufliegen, der einzige Bestimmungsfaktor für den Anteil der Köpfe an der Gesamtzugriffszeit. Dies ist durchschnittlich 0.0086 Millisekunden für eine Festplatte mit 10 000 Umdrehungen/Minute und 700 Sektoren pro Track.

5.4.1.3. Rotationsbedingte Latenz (Wartezeit)

Da sich die die Platten der Festplatte ständig drehen, ist es ziemlich unwahrscheinlich, dass die Platte sich genau am richtigen Punkt befindet, wenn die I/O-Anfrage eingeht, um auf den gewünschten Sektor zuzugreifen. Deshalb ist es, auch wenn die Festplatte bereit ist auf den Sektor zuzugreifen, für alles andere notwendig zu warten während sich die Platte dreht, um den gewünschten Sektor unter dem Lese/Schreib-Kopf zu positionieren.

Aus diesem Grund rotieren Hochleistungs-Festplatten deren Platten in einer höheren Geschwindigkeit. Heutzutage sind Geschwindigkeiten von 15.000 Umdrehungen/Minute für Höchstleistungs-Festplatten reserviert, während 5.400 U/min für einfache Festplatten als ausreichend gesehen werden. Durchschnittlich ergibt dies einen Wert von ungefähr 3 Millisekunden für eine Festplatte mit 10.000 U/min.

5.4.1.4. Bewegung des Zugriffsarms

Die Komponente einer Festplatte, die als Achillesferse angesehen werden kann, ist der Zugriffsarm. Der Grund dafür ist, dass der Zugriffsarm sich schnell und exakt über relativ weite Entfernungen hinweg bewegen muss. Zusätzlich dazu ist die Bewegung nicht kontinuierlich — der Arm muss beschleunigen, um den gewünschten Zylinder zu erreichen und dann schnell wieder abbremsen, um

nicht über das Ziel hinauszuschießen. Daher muss der Arm gleichzeitig kompakt (um den gewaltigen Kräften standzuhalten, die für die Beschleunigung notwenig sind) und leicht (damit weniger Masse beschleunigt/gebremst werden muss) sein.

Das Erreichen dieser wiedersprüchlichen Ziele ist schwierig. Dies wird tatsächlich auch durch die relativ lange Zeit bestätigt, die der Zugriffsarm im Gegensatz zu anderen Komponenten benötigt. Aus diesem Grund ist die Bewegung des Zugriffsarms der Hauptentscheidungsfaktor in puncto Gesamt-Performance der Festplatte, bei einem Durchschnittswert von circa 5,5 Millisekunden.

5.4.2. I/O-Lasten und Performance

Der andere Faktor, der die Performance der Festplatte steuert, ist die I/O-Last, der die Festplatte unterliegt. Einige der spezifischen Aspekte der I/O-Last sind:

- Menge der gelesenen Daten versus der geschriebenen Daten
- Die Anzahl der aktuellen Lese-/Schreibköpfe
- Die Lokalität der Lese-/Schreib-Daten

Diese werden in den folgenden Abschnitten genauer beschrieben.

5.4.2.1. Lesen versus Schreiben

Normale Festplatten mit magnetischen Medien als Datenspeicher sind vom Problem der Lese-Prozesse versus der Schreib-Prozesse weniger betroffen, da das Lesen und Schreiben die gleiche Zeit in Anspruch nimmt[6]. Andere Massenspeichergeräte benötigen jedoch unterschiedlich lange für das Verarbeiten von Lese- und Schreibaufgaben[7].

Dies hat zur Folge, dass Geräte, die länger zur Verarbeitung von Schreib-Aufgaben (zum Beispiel) benötigen, weniger Schreib-Aufgaben als Lese-Aufgaben verarbeiten können. Von einem anderen Gesichtspunkt aus betrachtet, benötigt eine Schreib-I/O mehr der Gerätefähigkeit zum Verarbeiten von I/O-Anfragen als eine Lese-I/O.

5.4.2.2. Mehrfache Lese-/Schreib-Anfragen

Eine Festplatte, die I/O-Anfragen von mehreren Quellen bearbeitet, erfährt eine andere Last als eine Festplatte, die nur Anfragen von einer Quelle verarbeitet. Der Hauptgrund dafür liegt in der Tatsache, dass mehrere I/O-Requester potentiell höhere I/O-Lasten auf einer Festplatte erzeugen als I/O-Anfragen von einer einzigen Quelle.

Dies liegt daran, dass der I/O-Requester einiges an Prozessleistung aufbringen muss, bevor eine I/O stattfinden kann. Schließlich muss der Requester die Art der I/O-Anfrage feststellen, bevor diese durchgeführt werden kann. Da die nötige Verarbeitung für diese Feststellung Zeit in Anspruch nimmt, gibt es eine Obergrenze für die I/O-Last, die ein jeder Requester generieren kann — nur eine schnellere CPU kann diese Grenze erhöhen. Diese Grenze wird eindeutiger, wenn zusätzlich dazu eine menschliche Eingabe verlangt wird.

---

6. Dies ist eigentlich nicht ganz richtig. Alle Festplatten besitzen eine bestimmte Menge an integriertem Cache-Speicher, der für die Verbesserung der Lese-Performance verwendet wird. Auf jede I/O-Anfrage für das Lesen muss jedoch mit dem eigentlichen physikalischen Lesen der Daten vom Speichermedium reagiert werden. Dies bedeutet, dass während der Cache die I/O-Leistungsprobleme ausgleichen kann, es doch niemals die Zeit, die für das physikalische Lesen der Daten benötigt wird, eliminieren kann.
7. Einige optische Festplatten zeigen dieses Verhalten aufgrund der physikalischen Einschränkungen der Technologien, die für die Implementierung der optischen Datenspeicherung nötig sind.

Mit mehreren Requestern können jedoch höhere I/O-Lasten getragen werden. Solange genügend CPU-Leistung vorhanden ist, um die Verarbeitung zum Generieren der I/O-Anfragen zu unterstützen, erhöht das Hinzufügen von weiteren I/O-Anfragern die I/O-Last.

Es gibt jedoch noch einen weiteren Aspekt, der Einfluss auf die I/O-Last hat. Dieser wird im folgenden Abschnitt beschrieben.

5.4.2.3. Lokalität der Lese-/Schreib-Daten

Auch wenn nicht streng an eine Multi-Requester-Umgebung gebunden, zeigt sich doch dieser Aspekt der Festplatten-Performance eher in solchen Umgebungen. Die Kernfrage ist, ob die I/O-Anfragen an eine Festplatte für Daten sind, die physikalisch nahe den anderen Daten liegen, die ebenso angefragt werden.

Der Grund hierfür wird klar, wenn man die elektro-mechanische Natur der Festplatte betrachtet. Die langsamste Komponente jeder Festplatte ist der Zugriffsarm. Wenn also auf Daten der eingehenden I/O-Anfragen zugegriffen wird und dies keine Bewegung des Zugriffsarms erfordert, kann die Festplatte wesentlich mehr I/O-Anfragen bearbeiten, als wenn die Daten über die gesamte Festplatte verteilt sind; was erheblich mehr Bewegungen des Zugriffsarms benötigt.

Dies wird deutlicher, wenn Sie sich die Festplatten-Performance ansehen. Diese Merkmale enthalten häufig *'angrenzende Zylinder'-Suchzeiten* (bei denen der Zugriffsarm nur ein klein wenig bewegt wird — nur bis zum nächsten Zylinder) und *'Full-Stroke'-Suchzeiten* (bei denen der Zugriffsarm vom ersten Zylinder bis hin zum letzten Zylinder bewegt wird). Hier zum Beispiel finden Sie die Suchzeiten für eine Hochleistungs-Festplatte:

Angrenzender Zylinder	Full-Stroke
0,6	8,2

Tabelle 5-4. Suchzeiten für angrenzende Zylinder und Full-Stroke/Gesamtzugriff (Lesekopf fährt quer über die Platte) (in Millisekunden)

5.5. Den Speicher nutzbar machen

Auch wenn ein Massenspeichergerät eingerichtet wurde, gibt es wenig, was man damit tun kann. Sicher können Daten auf dieses geschrieben und von diesem gelesen werden, ohne Struktur ist der Datenzugriff jedoch nur über Sektorenadressen (geometrisch oder logisch) möglich.

Es werden daher Methoden benötigt, mit denen der Speicher einer Festplatte leichter verwendbar wird. In den folgenden Abschnitten werden einige häufig eingesetzte Techniken genau zu diesem Thema erläutert.

5.5.1. Partitionen/Slices

Das erste, was einem Systemadministrator ins Auge fällt, ist die Tatsache, dass die Größe der Festplatte häufig die für die zu erledigende Aufgabe bei weitem übersteigt. Daher besitzen viele Betriebssysteme die Fähigkeit, den Speicherplatz einer Festplatte in verschiedene *Partitionen* oder *Slices* aufzuteilen.

Da diese getrennt von einander sind, können Partitionen verschieden groß sein, wobei der verwendete Speicherplatz keineswegs den Platz der anderen Partitionen raubt. So ist zum Beispiel die Partition, welche die Dateien für das Betriebssystem enthält, nicht betroffen, selbst wenn die Partition mit

den Benutzerdaten voll ist. Das Betriebssystem hat weiterhin genügend Speicherplatz für die eigene Verwendung.

Auch wenn dies sehr simpel erscheint, so können Sie Partitionen ähnlich wie eigene Festplatten betrachten. Und tatsächlich werden bei einigen Betriebssystemen Partitionen als "Laufwerke" bezeichnet. Diese Ansicht ist jedoch nicht ganz richtig; aus diesem Grund werden wir Partitionen im folgenden Abschnitt genauer betrachten.

5.5.1.1. Partitionsattribute

Partitionen werden durch folgende Attribute definiert:

- Partitionsgeometrie
- Partitionstyp
- Partitions-Typenfeld

Diese Attribute werden in den folgenden Abschnitten eingehender behandelt.

5.5.1.1.1. Geometrie

Die Geometrie einer Partition bezieht sich auf die physikalische Platzierung auf einer Festplatte. Die Geometrie kann hinsichtlich Start- und Endzylinder, Köpfe und Sektoren spezifiziert werden. Die meisten Partitionen beginnen und enden jedoch an Zylindergrenzen. Die Größe der Partition wird danach als die Menge des Speichers zwischen Start- und Endzylinder definiert.

5.5.1.1.2. Partitionstyp

Der Partitionstyp bezieht sich auf das Verhältnis der Partition zu den anderen Partitionen auf der Festplatte. Es gibt drei verschiedene Partitionstypen:

- Primär-Partitionen
- Erweiterte Partitionen
- Logische Partitionen

Im folgenden Abschnitt wird jeder Partitionstyp näher beschrieben.

5.5.1.1.2.1. Primär-Partitionen

Primär-Partitionen sind Partitionen, die einen der ersten vier Partitionierungs-Plätze in der Partitionierungstabelle der Festplatte belegen.

5.5.1.1.2.2. Erweiterte Partitionen

Erweiterte Partitionen wurden als Antwort auf den Bedarf an mehr als vier Partitionen pro Festplatte entwickelt. Eine erweiterte Partition kann selbst mehrere Partitionen enthalten, was die Anzahl der möglichen Partitionen auf einer Festplatte wesentlich erhöht. Die Einführung von erweiterten Partitionen wurde angetrieben durch die stetig wachsenden Fähigkeiten neuer Laufwerke.

5.5.1.1.2.3. Logische Partitionen

Logische Partitionen sind solche, die sich innerhalb einer erweiterten Partition befinden. Von der Verwendung her funktionieren diese nicht anders als nicht-erweiterte Primär-Partitionen.

5.5.1.1.3. Partitions-Typenfeld

Jede Partition besitzt ein Typenfeld, das einen Code für die erwartete Verwendung der Partition enthält. Dieses Typenfeld kann das Betriebssystem wiederspiegeln oder auch nicht. Anstelledessen kann es wiederspiegeln, wie Daten innerhalb der Partition gespeichert werden sollen. Im folgenden Abschnitt finden Sie weitere Informationen zu diesem wichtigen Punkt.

5.5.2. Dateisysteme

Selbst mit dem richtigen Massenspeichergerät, das richtig konfiguriert und angemessen partitioniert ist, sind wir immer noch nicht in der Lage, Informationen einfach zu speichern und abzurufen — wir haben immer noch keinen Weg gefunden, diese Daten zu strukturieren und zu organisieren. Was wir jetzt brauchen ist ein *Dateisystem*.

Das Konzept eines Dateisystems ist so fundamental für die Verwendung von Massenspeichergeräten, dass der durchschnittliche Computerbenutzer meistens diese nicht unterscheidet. Systemadministratoren können es sich nicht leisten, Dateisysteme und deren Einfluss auf die tägliche Arbeit zu ignorieren.

Ein Dateisystem ist eine Methode, Daten auf einem Massenspeichergerät zu präsentieren. Dateisysteme enthalten normalerweise die folgenden Eigenschaften:

- Datei-basierte Datenspeicherung
- Hierarchische Verzeichnisstruktur (manchmal auch als "Folder" oder Ordner bezeichnet)
- Verfolgen der Dateierstellungs-, Zugangs- und Änderungsdaten
- Ein gewisser Grad an Kontrolle über die Art des Zugangs zu bestimmten Dateien
- Dateibesitz-Begriff (Ownership)
- Haushaltung des verfügbaren Speicherplatzes

Nicht alle Dateisysteme besitzen alle diese Eigenschaften. Ein Dateisystem zum Beispiel, das für ein Einzelbenutzersystem entwickelt wurde, kann einfach eine simplere Methode der Zugangskontrolle verwenden und auf Dateibesitzermerkmale ganz verzichten.

Sie sollten jedoch dabei im Hinterkopf behalten, dass ein Dateisystem einen großen Einfluss auf Ihre tägliche Arbeit haben kann. Indem Sie sicherstellen, dass das von Ihnen verwendete Dateisystem den funktionalen Anforderungen Ihres Unternehmens entspricht, sorgen Sie nicht nur dafür, dass das Dateisystem den Aufgaben gewachsen ist, sondern auch dass es einfach und effizient zu verwalten ist.

Vor diesem Hintergrund werden die Eigenschaften in den folgenden Abschnitten näher beschrieben.

5.5.2.1. Datei-basierte Speicherung

Während Dateisysteme, welche die Datei-Metapher für die Datenspeicherung verwenden schon so weitverbreitet sind, dass diese als gegeben angesehen werden können, gibt es doch einige Aspekte, die hier ins Auge gefasst werden sollen.

Zuallererst müssen Sie Einschränkungen der Dateinamen beachten. Welche Zeichen darf z.B. ein Dateiname enthalten? Wie lang darf dieser Dateiname sein? Diese Fragen sind wichtig, da durch sie die Dateinamen bestimmt werden, die verwendet werden dürfen. Ältere Betriebssysteme mit primitiven

Dateisystemen erlauben häufig nur alphanumerische Zeichen (und nur in Großbuchstaben) und nur traditionelle *8.3* Dateinamen (d.h. ein acht-Zeichen langer Dateiname gefolgt von einer 3-Zeichen Dateierweiterung).

5.5.2.2. Hierarchische Verzeichnisstruktur

Während Dateisysteme in ganz alten Betriebssystemen das Konzept der Verzeichnisse nicht enthielten, verwenden alle allgemein verwendeten modernen Dateisysteme diese Eigenschaft. Verzeichnisse selbst werden gewöhnlich als Dateien implementiert, was bedeutet, dass keine bestimmten Dienstprogramme für deren Wartung benötigt werden.

Desweiteren können Verzeichnisse, da diese selbst Dateien darstellen und Verzeichnisse Dateien enthalten, auch andere Verzeichnisse enthalten, was eine vielschichtige Verzeichnisstruktur ermöglicht. Dies ist ein leistungsstarkes Konzept, mit dem alle Systemadministratoren vertraut sein sollten. Vielschichtige Verzeichnishierarchien können die Dateiverwaltung erheblich für Sie und für Ihre Benutzer erleichtern.

5.5.2.3. Nachverfolgen der Dateierstellungs-, Zugangs- und Modifizierungszeiten

Die meisten Dateisysteme verfolgen den Zeitpunkt, an dem eine Datei erstellt wurde; manche verfolgen auch die Änderungs- und Zugriffszeiten. Abgesehen von der Bequemlichkeit feststellen zu können, wann eine Datei erstellt, geöffnet oder geändert wurde, sind diese Daten wichtig für die richtige Durchführung inkrementeller Backups.

Weitere Informationen über die Verwendung dieser Dateisystem-Eigenschaften für Backups finden Sie unter Abschnitt 8.2.

5.5.2.4. Zugriffskontrolle

Zugriffskontrolle ist ein Bereich, in dem sich Dateisysteme erheblich unterscheiden. Einige Dateisysteme haben keine klaren Modelle für die Zugriffskontrolle, während andere wesentlich weiter entwickelt sind. Im Allgemeinen kombinieren die meisten modernen Dateisysteme zwei Komponenten in einer Zugriffskontroll-Methodologie:

- Benutzeridentifikation
- Benutzerberechtigungen-Liste

Benutzeridentifikation bedeutet, dass das Dateisystem (und das darunterliegende Betriebssystem) in der Lage sein muss, individuelle Benutzer eindeutig zu identifizieren. Dies macht es möglich, volle Verantwortlichkeit für alle Vorgänge in Hinsicht auf Tätigkeiten auf Dateisystemebene zu besitzen. Eine weiteres oft hilfreiches Feature ist das der Benutzer-*Gruppen* — ad-hoc Sammlungen von Benutzern. Gruppen werden am häufigsten von Unternehmen verwendet, in denen Benutzer an einem oder mehreren Projekten mitarbeiten. Eine weitere von einigen Dateisystemen unterstützte Eigenschaft ist die Erstellung von allgemeinen Kennungen, die an einen oder an mehrere Benutzer vergeben werden können.

Desweiteren muss das Dateisystem in der Lage sein, Listen von berechtigten Aktivitäten (oder auch nicht-berechtigten Aktivitäten in Bezug auf jede einzelne Datei zu prüfen. Die am häufigsten nachverfolgten Aktivitäten sind:

- Lesen der Datei
- Schreiben der Datei
- Ausführen der Datei

Verschiedene Dateisysteme können diese Listen eventuell auch erweitern, indem auch andere Aktivitäten wie das Löschen oder die Fähigkeit Änderungen an den Zugangskontrollen einer Datei durchführen zu können, inkludiert werden können.

5.5.2.5. Haushaltung des verfügbaren Speicherplatzes

Eine Konstante im Leben eines Systemadministrators ist, dass es niemals genug freien Speicherplatz gibt. Und selbst wenn, bleibt dieser nicht lange frei. Daher sollte ein Systemadministrator zumindest in der Lage sein, die Menge an freiem Speicherplatz für jedes Dateisystem festlegen zu können. Zusätzlich dazu enthalten Dateisysteme mit wohldefinierten Benutzeridentifikations-Fähigkeiten die Möglichkeit, den Speicher anzuzeigen, den ein bestimmter Benutzer verwendet hat.

Dieses Feature ist lebensnotwendig für große Mehrplatz-Umgebungen, da auch hier leider nur allzuoft die 80/20 Regel für Festplattenplatz gilt — 20 Prozent der Benutzer verbrauchen 80 Prozent des verfügbaren Speicherplatzes. In dem Sie es möglichst einfach gestalten, genau diese 20 Prozent ausfindig machen zu können, können Sie effektiver Ihre speicherbezogenen Bestände verwalten.

Weiters besitzen einige Dateisysteme die Möglichkeit, ein bestimmtes Limit pro Benutzer (auch bekannt als *Festplattenquote*) für den verwendeten Festplattenplatz festzulegen. Diese Spezifikationen unterscheiden sich von Dateisystem zu Dateisystem. Im Allgemeinen kann Benutzern eine bestimmte Menge Speicher zugewiesen werden, welche diese dann verwenden können. Darüberhinaus unterscheiden sich einige Dateisysteme voneinander. Manche erlauben dem Benutzer, diese Grenze einmalig zu überschreiten, während andere eine "Gnadenfrist" setzen, in der ein zweites, etwas höheres Limit für diesen Zeitraum gilt.

5.5.3. Verzeichnisstruktur

Viele Systemadministratoren denken nur wenig darüber nach, wie der heute an Benutzer vergebene Speicher, morgen eingesetzt wird. Wenn Sie jedoch einige Überlegungen anstellen, bevor Sie Speicher an Benutzer vergeben, können Sie sich selbst eine ziemliche Menge an späterer Arbeit ersparen.

Das Wichtigste, das ein Systemadministrator tun kann, ist Verzeichnisse und Unterverzeichnisse dazu zu verwenden, den Speicher auf eine verständlich Art und Weise zu strukturieren. Diese Vorgehensweise bringt einige Vorteile mit sich:

- Einfacher zu verstehen
- Mehr Flexibilität in der Zukunft

Indem Sie Struktur in den Speicher bringen, ist dieser auch leichter zu verstehen. Betrachten Sie zum Beispiel ein großes System mit vielen Benutzern. Anstelle das Sie alle Benutzerverzeichnisse in einem großen Verzeichnis ablegen, ergibt es mehr Sinn, wenn Sie Unterverzeichnisse verwenden, die die Struktur Ihres Unternehmens wiederspiegeln. Auf diese Weise haben z.B. die Mitarbeiter in der Buchhaltung ihre eigenen Verzeichnisse unter einem Verzeichnis mit dem Namen `Buchhaltung` und Mitarbeiter in der Engineering-Abteilung deren Verzeichnisse unter `Engineering` und so weiter.

Die Vorteile einer solchen Vorgehensweise sind, dass es auf einer tagtäglichen Basis leichter wäre, den jeweiligen Speicherbedarf (und -Nutzung) für jeden Bereich des Unternehmens nachzuverfolgen. Eine Liste aller Dateien zu bekommen, die von jedem in der Personalabteilung verwendet werden, ist relativ einfach. Ein Backup aller Dateien in der Rechtsabteilung zu erstellen, wird dadurch ebenfalls leicht gemacht.

Durch eine geeignete Struktur wird gleichzeitig die Flexibilität erhöht. Um das vorherige Beispiel fortzusetzen, nehmen wir einmal an, dass die Entwicklungsabteilung mehrere neue Projekte übernimmt. Aufgrunddessen werden zukünftig viele neue Entwickler eingestellt. Es gibt zur Zeit jedoch nicht genügend Speicherplatz, um das erwartete Wachstum in der Entwicklungsabteilung abzudecken.

Da jedoch alle Dateien aller Personen in der Entwicklungsabteilung unter dem Verzeichnis`Engineering` abgelegt sind, wäre es relativ einfach::

- Den zusätzlichen benötigten Speicherplatz zu schaffen
- Ein Backup aller Daten unter dem Verzeichnis `Engineering` durchzuführen
- Das Backup auf dem neuen Speicher wiederherzustellen
- Das Verzeichnis `Engineering` auf dem ursprünglichen Speicher in etwas wie z.B. `Engineering-Archiv` umzubenennen (bevor dies vollständig gelöscht wird, nachdem die neue Konfiguration einen Monat lang einwandfrei funktioniert hat)
- Die nötigen Änderungen durchzuführen, so dass alle Mitarbeiter inEngineering auf die Dateien im neuen Speicher zugreifen können

Dieser Ansatz hat sicherlich auch einige Nachteile. Wenn zum Beispiel Mitarbeiter häufig die Abteilung wechseln, müssen Sie einen Weg finden, hierüber informiert zu bleiben, um die Verzeichnisstruktur entsprechend ändern zu können. Ansonsten entspricht diese Struktur nicht mehr länger der Realität, was langfristig gesehen zu mehr — und nicht weniger — Arbeit für Sie führt.

5.5.4. Speicherzugang ermöglichen

Sobald ein Massenspeichergerät richtig partitioniert und ein Dateisystem angelegt wurde, kann der Speicher allgemein verwendet werden.

Bei einigen Betriebssystemen ist dies möglich. Sobald das Betriebssystem das neue Massenspeichergerät erkannt hat, kann dies vom Systemadministrator formatiert und sofort ohne weiteren Aufwand verwendet werden.

Andere Betriebssysteme benötigen einen weiteren Schritt. Dieser Schritt — häufig als *Mounting* bezeichnet — weist das Betriebssystem an, wie auf den Speicher zugegriffen werden darf. Das Mounten von Speicher wird gewöhnlich mittels einem speziellem Utility-Programm oder Befehl ausgeführt und erfordert die ausdrückliche Identifizierung des Massenspeichergerätes (und eventuell der Partition).

5.6. Fortgeschrittene Speicher-Technologien

Auch wenn alles in diesem Kapitel soweit nur für einzelne Festplatten, die direkt mit einem System verbunden sind, beschrieben wurde, gibt es weitere, fortgeschrittene Optionen, die Sie untersuchen können. Die folgenden Abschnitte beschreiben einige der üblicheren Vorgehensweisen zur Erweiterung Ihrer Massenspeicher-Optionen.

5.6.1. Netzwerk-zugänglicher Speicher

Die Kombination von Netzwerk und Massenspeichergerät kann in wesentlich höherer Flexibilität für Systemadministratoren resultieren. Es gibt zwei eventuelle Vorteile, die diese Art der Konfiguration mit sich bringt:

- Zusammenlegung von Speicher
- Vereinfachte Verwaltung

Speicher kann durch den Einsatz von Hochleistungs-Servern mit Hochgeschwindigkeits-Netzwerkverbindungen und großer Menge schnellem Speicher zusammengelegt werden. Mit der richtigen Konfiguration ist es möglich, Speicherzugang mit Geschwindigkeiten, die mit lokal-verbundenem Speicher verglichen werden können, zu erreichen. Desweiteren ermöglicht die gemeinsame Verwendung solch einer Konfiguration Kosteneinsparungen, da die Ausgaben für

zentralisierten, gemeinsam verwendeten Speicher höchstwahrscheinlich geringer sind, als Speicher für jeden einzelnen Client. Zusätzlich dazu wird freier Speicherplatz zentral verwaltet, anstatt dass dieser über viele Clients verteilt ist (und daher nicht weitläufig verwendet werden kann).

Zentralisierte Speicher-Server können auch viele Verwaltungsaufgaben erleichtern. So ist zum Beispiel die Überwachung des freien Speicherplatzes wesentlich einfacher, wenn sich der zu überwachende Speicher auf einem zentralisierten Speicher-Server befindet. Auch Backups können unter diesem Umstand stark vereinfacht werden. Es gibt die Möglichkeit netzwerkfähiger Backups für mehrere Clients, wobei dies jedoch mehr Arbeit in der Konfiguration und Verwaltung bedeutet.

Es gibt eine Reihe von verschiedenen Netzwerk-Speichertechnologien. Die entsprechende Auswahl kann sich daher schwierig gestalten. Fast jedes heute erhältliche Betriebsystem enthält eine Vorrichtung für das Zugreifen auf Netzwerk-zugänglichen Speicher, wobei die verschiedenen Technologien jedoch untereinander nicht kompatibel sind. Was ist nun die beste Vorgehensweise bei der Entscheidung welche der Technologien letztendlich eingesetzt werden soll?

Für gewöhnlich erhalten Sie die besten Resultate, wenn Sie die eingebauten Leistungsfähigkeiten des Clients diese Frage entscheiden zu lassen. Hierfür gibt eine Reihe von Gründen:

- Minimale Client-Integrationsprobleme
- Minimaler Aufwand für jedes der Client-Systeme
- Geringe Kosten pro Client

Denken Sie daran, dass sich alle Client-bezogenen Probleme relativ zu der Anzahl der Clients in Ihrem Unternehmen vergrößern. In dem Sie die integrierten Fähigkeiten der Clients nutzen, müssen Sie keine zusätzliche Software auf jedem Client installieren (und somit entstehen auch keinerlei Kosten in Zusammenhang mit Software-Beschaffung).

Es gibt jedoch einen Nachteil. Dies bedeutet, dass die Serverumgebung in der Lage sein muss, gute Unterstützung für die von den Clients benötigten Netzwerk-zugänglichen Speicher-Technologien zu bieten. In Fällen wo der Server und Client-Betriebssysteme ein und dasselbe sind, gibt es normalerweise keine Probleme. Ansonsten müssen Sie Zeit und Mühe investieren, damit der Server die Sprache des Clients "spricht". Diese gegenseitige Abstimmung ist häufig jedoch mehr als gerechtfertigt.

5.6.2. RAID-basierter Speicher

Eine Fertigkeit, die ein Systemadministrator kultivieren sollte, ist die Fähigkeit komplexe Systemkonfigurationen zu betrachten und dabei die jeweils inhärenten Unzulänglichkeiten und Mängel der jeweiligen Konfiguration feststellen zu können. Während dies ein auf den ersten Blick eher deprimierender Standpunkt zu sein scheint, kann es doch eine gute Art und Weise darstellen, hinter die Fassade der neuen, glänzenden Verpackungen zu schauen und sich vorzustellen, dass an irgendeiner zukünftigen Samstag Nacht die komplette Produktion zusammenbricht, aufgrund eines Fehlers, der einfach durch ein wenig vorausschauendes Planen hätte vermieden werden können.

Mit diesen Informationen im Hinterkopf lassen Sie uns nun unser Wissen über Festplatten-basierten Speicher anwenden und sehen, ob wir feststellen können, auf welche Arten Festplatten Probleme bereiten können. Denken Sie zuallererst an einen gänzlichen Hardwareausfall:

Eine Festplatte mit vier Partitionen bricht vollständig zusammen: was passiert mit den Daten auf diesen Partitionen?

Daten sind unmittelbar nicht mehr verfügbar (zumindest bis die ausgefallene Einheit ersetzt und die Daten von einem Backup wiederhergestellt wurden).

Eine Festplatte mit einer einzigen Partition hat ihre Leistungsgrenzen aufgrund massiver I/O-Lasten erreicht: was passiert mit Applikationen, die auf die Daten auf dieser Partition zugreifen müssen?

Die Applikationen werden langsamer, da die Festplatte Lese- und Schreibvorgänge nicht schneller bearbeiten kann.

Sie haben eine große Datei, die langsam wächst. Demnächst wird diese größer sein als die größte Festplatte in Ihrem System. Was passiert dann?

Die Festplatte füllt sich, die Datei kann nicht weiter wachsen und die damit verbundenen Applikationen können nicht weiterlaufen.

Nur eines dieser Probleme kann ein Datenzentrum zum Stillstand bringen. Systemadministratoren begegnen diesen Problemen jedoch auf nahezu täglicher Basis. Was kann getan werden?

Glücklicherweise gibt es eine Technologie, die auf jedes dieser Probleme eingeht. Die Bezeichnung für diese Technologie ist *RAID*.

5.6.2.1. Grundkonzepte

RAID ist ein Akronym für Redundant Array of Independent Disks[8]. Wie der Name impliziert ist RAID eine Methode, mehrere Festplatten als eine Festplatte verhalten zu lassen.

RAID-Technologien wurden zuerst von Wissenschaftlern an der Berkeley Universität von Kalifornien Mitte der 80er Jahre entwickelt. Damals gab es einen großen Preisunterschied zwischen den Hochleistungs-Festplatten der damaligen großen Computersysteme und den kleineren Festplatten, die von der noch jungen PC-Industrie verwendet wurden. RAID wurde als eine Methode angesehen, mehrere kostengünstige Festplatten an Stelle einer hochpreisigen Einheit einzusetzen.

Wichtiger noch, RAID Arrays können auf verschiedene Weise zusammengesetzt werden, was zu verschiedenen Charakteristika, abhängig von der endgültigen Konfiguration, führt. Lassen Sie uns nun einen genaueren Blick auf die verschiedenen Konfigurationen (auch bekannt als RAID-*Levels*) werfen.

5.6.2.1.1. RAID-Levels

Die Berkeley-Wissenschaftler definierten ursprünglich fünf verschiedene RAID-Level und nummerierten diese von "1" bis "5". Mit der Zeit wurden zusätzliche RAID-Level von anderen Forschern und Mitgliedern der Speicherindustrie definiert. Nicht alle RAID-Level waren gleich nützlich; einige waren nur für Forschungszwecke sinnvoll und andere konnten vom ökonomischen Standpunkt aus nicht implementiert werden.

Zum Schluss gab es drei RAID-Level, die weitverbreitete Anwendung fanden:

- Level 0
- Level 1
- Level 5

In den folgenden Abschnitten werden diese Level im Detail beschrieben.

5.6.2.1.1.1. RAID 0

Die Festplattenkonfiguration, die als RAID-Level 0 bekannt ist, ist leicht irreführend, da dieser Level als einziger RAID-Level gar keine Redundanz verwendet. Auch wenn RAID 0 keine Vorteile vom Blickpunkt der Verlässlichkeit besitzt, hat es doch andere Vorteile.

Ein RAID 0 Array besteht aus zwei oder mehr Festplatten. Die verfügbare Speicherkapazität ist aufgeteilt in *Chunks*, die ein Vielfaches der nativen Blockgröße der Festplatte darstellen. Daten, die auf dieses Array geschrieben werden, werden Chunk für Chunk auf jede Festplatte im Array geschrieben.

8. In den Anfängen der RAID-Forschung stand das Akronym für Redundant Array of *Inexpensive* Disks, über Zeit jedoch wurden die "Standalone" Festplatten, die RAID ersetzen sollte, immer günstiger und machten so den Verweis auf den Preis bedeutungslos.

Die Chunks können als Streifen (Stripes) über jede Festplatte im Array betrachtet werden; daher der andere Name für RAID 0: *Striping*.

Wenn zum Beispiel 12KB Daten mit einem zwei-Festplatten Array und einer 4KB Chunk-Größe auf das Array geschrieben werden, werden diese Daten in jeweils drei 4KB Chunks auf die folgenden Festplatten geschrieben:

- Die ersten 4KB werden auf die erste Festplatte, in den ersten Chunk geschrieben
- Die zweiten 4KB werden auf die zweite Festplatte, in den ersten Chunk geschrieben
- Die dritten 4KB werden auf die erste Festplatte, in den zweiten Chunk geschrieben

Im Vergleich zu einer einzigen Festplatte umfassen die Vorteile von RAID 0 folgende:

- Größere Gesamtgröße — RAID 0 Arrays können so konstruiert werden, dass diese größer sind, als eine einzige Festplatte, was das Speichern von größeren Datendateien ermöglicht
- Bessere Lese-/Schreib-Performance — Die I/O-Last auf einem RAID 0 Array wird gleichmäßig über alle Festplatten im Array verteilt (davon ausgehend, dass alle I/O sich nicht auf einen einzigen Chunk konzentrieren)
- Kein verschwendeter Speicherplatz — Der gesamte verfügbare Speicher auf allen Festplatten im Array kann für das Speichern von Daten verwendet werden

Im Vergleich zu einer einzigen Festplatte hat RAID 0 folgende Nachteile:

- Geringere Verlässlichkeit — Jede Festplatte in einem RAID 0 Array muss funktionieren, damit das Array verfügbar ist; ein Ausfall einer Festplatte in einem RAID 0 Array mit N Festplatten hat zur Folge, dass $1/N$tel aller Daten nicht zur Verfügung steht, was das Array nutzlos macht

Tipp

Wenn Sie Probleme haben, die verschiedenen RAID-Level zu unterscheiden, denken Sie daran, dass RAID 0 *Null* Prozent Redundanz hat.

5.6.2.1.1.2. RAID 1

RAID 1 verwendet zwei (auch wenn einige Implementierungen mehr unterstützen) identische Festplatten. Alle Daten werden auf zwei Festplatten geschrieben, die so zu einem Spiegelbild von sich selbst werden. Aus diesem Grund wird RAID 1 häufig auch als *Mirroring* bezeichnet.

Sobald Daten auf ein RAID 1 Array geschrieben werden, müssen zwei physikalische Schreibvorgänge stattfinden: einer für die erste und einer für die zweite Festplatte. Das Lesen von Daten findet im Gegensatz dazu nur einmal statt und jede der Festplatten im Array kann dazu verwendet werden.

Im Vergleich zu einer einzigen Festplatte hat eine RAID 1 Array folgende Vorteile:

- Verbesserte Redundanz —Auch wenn eine Festplatte im Array vollständig ausfällt, können die Daten weiterhin abgerufen werden
- Verbesserte Lese-Performance — Sind beide Festplatten funktionsfähig, können Lesevorgänge gleichmäßig aufgeteilt werden, was die I/O-Last reduziert

Im Vergleich zu einer einzigen Festplatte hat ein RAID 1 Array folgende Nachteile:

- Die maximale Array-Größe ist beschränkt auf die Größe der größten Festplatte.

- Reduzierte Schreib-Performance — Da beide Festplatten aktuell gehalten werden müssen, müssen alle Schreib-I/Os auf beiden Festplatten durchgeführt werden, was den gesamten Vorgang des Schreibens der Daten verlangsamt
- Höhere Kosten — Da eine gesamte Festplatte für Redundanz bereitsteht, sind die Kosten für ein RAID 1 Array mindestens doppelt so hoch wie die für eine einzelne Festplatte

Tipp

Wenn Sie Probleme haben, die verschiedenen RAID-Level zu unterscheiden, denken Sie daran, dass RAID 1 *ein*hundert Prozent Redundanz besitzt.

5.6.2.1.1.3. RAID 5

RAID 5 versucht die Vorteile von RAID 0 und RAID 1 zu kombinieren und deren Nachteile zu minimieren.

Wie RAID 0 besteht auch RAID 5 aus mehreren Festplatten, die jeweils in Chunks unterteilt sind. Dies ermöglicht einem RAID 5 Array, größer zu sein als eine einzelne Festplatte, Wie RAID 1 Arrays verwendet ein RAID 5 Array einigen Festplattenplatz auf redundante Weise, was die Zuverlässigkeit verbessert.

Die Funktionsweise von RAID 5 unterscheidet sich jedoch von RAID 0 oder 1.

Ein RAID 5 Array muss aus mindestens drei identischen Festplatten bestehen (es können jedoch mehr Festplatten verwendet werden). Jede Festplatte ist in Chunks unterteilt und Daten werden der Reihe nach auf diese Chunks geschrieben. Nicht jeder Chunk ist jedoch auf die Speicherung von Daten wie in RAID 0 ausgelegt. Stattdessen wird in einem Array mit n Festplatten jeder $n$te Chunk für die *Parität* verwendet.

Chunks, die eine Parität enthalten, ermöglichen das Wiederherstellen von Daten, falls eine Festplatte im Array ausfällt. Die Parität im Chunk x wird durch eine mathematische Kombination aller Daten in jedem Chunk x auf allen Festplatten im Array errechnet. Werden Daten in einem Chunk aktualisiert, muss der entsprechende Paritätsblock ebenfalls neu kalkuliert und aktualisiert werden.

Dies bedeutet, dass jedes Mal, wenn Daten auf das Array geschrieben werden, auf mindestens *zwei* Festplatten geschrieben wird: die Festplatte, die die Daten hält und die Festplatte, die den Paritätsblock enthält.

Ein Punkt, den Sie dabei im Auge behalten sollten, ist die Tatsache, dass die Paritätsblöcke sich nicht auf eine bestimmte Festplatte im Array konzentrieren. Stattdessen sind diese über alle Festplatten verteilt. Auch wenn es möglich ist, eine bestimmte Festplatte für die Parität zu reservieren (dies wird als RAID-Level 4 bezeichnet), bedeutet das kontinuierliche Aktualisieren der Parität, indem Daten auf das Array geschrieben werden, dass die Paritäten-Festplatte zu einem Performance-Engpass wird. Indem die Paritäts-Informationen gleichmäßig über das Array verteilt werden, wird dieser Einfluss verringert.

Die Auswirkung der Parität auf die Gesamt-Speicherkapazität des Arrays sollte dabei nicht außer Acht gelassen werden. Auch wenn die Paritäts-Informationen gleichmäßig über die Festplatten im Array verteilt werden, so wird die Größe des verfügbaren Speichers um die Größe einer Festplatte reduziert.

Im Vergleich zu einer einzigen Festplatte hat ein RAID 5 Array folgende Vorteile:

- Verbesserte Redundanz — Wenn eine Festplatte im Array ausfällt, können die Paritäts-Informationen zur Wiederherstellung der fehlenden Datenblöcke (Chunks) verwendet werden und dies während das Array weiterhin verwendet werden kann[9]
- Verbesserte Lese-Performance — Dadurch, dass Daten wie im RAID 0 über die Festplatten im Array verteilt werden, wird die Lese-I/O-Aktivität gleichmäßig über die Festplatten verteilt
- Relativ gute Kosteneffizienz — Für ein RAID 5 Array mit n Festplatten wird nur $1/n$tel des Gesamtspeichers der Redundanz gewidmet

Im Vergleich zu einer einzigen Festplatte hat ein RAID 5 Array folgende Nachteile:

- Verringerte Schreib-Performance — da das Schreiben auf das Array eigentlich zwei Schreibvorgänge auf die physikalischen Festplatten erfordert (einen für die Daten und einen für die Parität) ist die Schreib-Leistung schlechter als bei einer einzigen Festplatte[10]

5.6.2.1.1.4. Nested RAID-Level ('Zusammengesetzte' RAID-Level)

Wie bereits klar aus der Diskussion über die verschiedenen RAID-Level hervorgehen sollte, hat jedes Level bestimmte Stärken und Schwächen. Nicht lange nach dem erstmaligen Einsatz der RAID-basierten Speicher fragte man sich, ob die verschiedenen RAID-Level nicht irgendwie kombiniert werden könnten, um so Arrays mit allen Stärken und ohne die Schwächen der originalen Level zu erhalten.

Was zum Beispiel, wenn die Festplatten in einem RAID 0 Array eigentlich RAID 1 Arrays wären? Dies würde die Vorteile der RAID 0 Geschwindigkeit mit der Verlässlichkeit von RAID 1 vereinen.

Und dies ist genau das, was machbar ist. Hier die häufigsten Nested RAID-Level:

- RAID 1+0
- RAID 5+0
- RAID 5+1

Da Nested RAID in spezialisierteren Umgebungen eingesetzt wird, werden wir hier nicht näher ins Detail gehen. Es gibt jedoch zwei Punkte, die bei Nested RAID zu beachten sind:

- Reihenfolge ist wichtig — Die Reihenfolge, in der RAID-Level 'vernestet' werden hat einen großen Einfluss auf die Verlässlichkeit. Mit anderen Worten: RAID 1+0 und RAID 0+1 sind *nicht* das selbe.
- Höhere Kosten — Der Nachteil, den alle nested RAID-Implementierungen gemeinsam haben, sind die Kosten. So besteht z.B. das kleinstmögliche RAID 5+1 Array aus sechs Festplatten (für größere Arrays werden sogar noch mehr Festplatten benötigt).

Da wir nun die Begriffe rund um RAID eingehender betrachtet haben, befassen wir uns nun damit, wie RAID implementiert werden kann.

---

9. Wenn eine Festplatte ausfällt, wird aufgrund des Overhead, der durch das Wiederherstellen fehlender Daten erzeugt wird die I/O-Performance beeinträchtigt.
10. Nicht zu vergessen sind die Auswirkungen, die Paritäts-Kalkulationen haben, die für jeden Schreibvorgang benötigt werden. Abhängig von der jeweiligen RAID 5 Implementierung (insbesondere dort im System, wo die Paritäts-Kalkulationen stattfinden), kann jedoch das Ausmaß dieser Auswirkungen von messbar bis hin zu 'nahezu nicht vorhanden' reichen.

5.6.2.1.2. RAID-Implementierungen

Aus dem vorherigen Abschnitt wird klar, dass RAID zusätzliche "Intelligenz" über die gewöhnliche I/O-Verarbeitung individueller Festplatten hinauserfordert. Zumindest müssen folgende Aufgaben erfüllt werden:

- Aufteilen eingehender I/O-Anfragen an die einzelnen Festplatten im Array
- Für RAID 5 das Errechnen der Parität und das Schreiben auf die entsprechende Festplatte im Array
- Das Überwachen der einzelnen Festplatten im Array und das Ausführen der angemessenen Maßnahmen, sollte eine Festplatte ausfallen
- Die Kontrolle der Wiederherstellung einer individuellen Festplatte im Array, wenn diese ersetzt oder repariert wurde
- Das Bereitstellen von Maßnahmen, die den Administratoren die Wartung des Arrays ermöglichen (Hinzufügen und Löschen von Laufwerken, Wiederherstellung, etc.)

Es gibt zwei hautpsächliche Methoden, die zum Ausführen dieser Aufgaben verwendet werden können. In den nächsten beiden Abschnitten werden diese in größerem Detail beschrieben.

5.6.2.1.2.1. Hardware-RAID

Eine Hardware-RAID Implementierung wird normalerweise durch eine besondere Festplatten-Controller-Karte ausgeführt. Diese Karte führt alle RAID-bezogenen Funktionen aus und kontrolliert die einzelnen Festplatten direkt im Array. Mit dem richtigen Treiber werden die Arrays, die von einer Hardware-RAID-Karte verwaltet werden, dem Host-Betriebssystem so angezeigt, als wären dies reguläre Festplatten.

Die meisten RAID-Controller-Karten arbeiten mit SCSI-Laufwerken, es gibt jedoch auch einige ATA-basierte RAID-Controller. In jedem Fall wird die Verwaltungsoberfläche für gewöhnlich durch eine der drei folgenden Methoden implementiert:

- Durch spezialisierte Utility-Programme, die als Applikationen unter dem Hostsystem ausgeführt werden und so der Controller-Karte eine Software-Schnittstelle bieten
- Eine integrierte Schnittstelle, die einen seriellen Port verwendet, auf den über einen Terminal-Emulator zugegriffen wird
- Eine BIOS-artige Schnittstelle, die nur während dem Booten des Systems zur Verfügung steht

Einige RAID-Controller besitzen mehr als eine administrative Schnittstelle. Aus offensichtlichen Gründen bietet eine Software-Schnittstelle die größte Flexibilität, da administrative Funktionen ermöglicht werden während das Betriebssystem läuft. Wenn Sie jedoch ein Betriebssystem von einem RAID-Controller aus booten, ist die Voraussetzung eine Schnittstelle, die kein laufendes Betriebssystem benötigt.

Da es sehr viele verschiedene RAID-Controller-Karten auf dem Markt gibt, ist es uns nicht möglich, hierbei zu sehr ins Detail zu gehen. Für weitere Informationen sollten Sie sich daher an die Dokumentation des Herstellers halten.

5.6.2.1.2.2. Software-RAID

Software-RAID ist ein RAID System, welches als Kernel- oder Treiber-Software für ein bestimmtes Betriebssystem implementiert wurde. Als solches bietet es größere Flexibilität in Bezug auf Hardware-Support — solange die Hardware auch vom Betriebssystem unterstützt wird, können RAID Arrays konfiguriert und eingesetzt werden. Dies kann die Kosten eines RAID-Einsatzes wesentlich reduzieren, da kein Bedarf für kostenintensive, spezialisierte RAID-Hardware besteht.

Häufig übersteigt die überschüssige CPU-Leistung für Software-RAID-Paritätsberechnungen die Verarbeitungsleistung einer RAID-Controller-Karte. Aus diesem Grund unterstützen einige Software-RAID-Implementierungen eine höhere Performance als Hardware-RAID-Implementierungen.

Software-RAIDs haben jedoch Begrenzungen, die Hardware-RAID nicht besitzen. Die Wichtigste von allen ist die Unterstützung des Bootens von einem anderen Software-RAID Array. In den meisten Fällen können nur RAID 1 Arrays für das Booten verwendet werden, da das BIOS des Computers nicht auf RAID achtet. Da eine einzelne Festplatte von einem RAID 1 Array nicht von einem Nicht-RAID Boot-Gerät unterschieden werden kann, kann das BIOS den Bootprozess erfolgreich starten. Das Betriebssystem kann dann zum Software-RAID-Betrieb wechseln, sobald es Kontrolle über das System erlangt hat.

5.6.3. Logical Volume Management (LVM)

Eine weitere fortgeschrittene Speichertechnologie ist das *Logical Volume Management* (LVM). Mit LVM können Sie physikalische Massenspeichergeräte als Bausteine auf unterster Stufe behandeln, auf denen verschiedene Speicherkonfigurationen aufgebaut werden. Die jeweilige Leistungsfähigkeit variiert mit der jeweiligen Implementierung, können aber physikalische Speichergruppierung, logische Volumsänderung und Datenmigration beinhalten.

5.6.3.1. Physikalische Speichergruppierung

Auch wenn der Name, der dieser Fähigkeit verliehen wurde, etwas abweichen kann, ist die physikalische Speichergruppierung der Grundbaustein für alle LVM-Implementierungen. Wie der Name besagt, können die physikalischen Massenspeichergeräte so gruppiert werden, dass ein oder mehrere logische Massenspeichergeräte entstehen. Diese logischen Massenspeichergeräte (oder logische Volumen) können eine größere Kapazität besitzen, als irgendwelche der eigentlichen, physikalischen Massenspeichergeräte, die dem zugrunde liegen.

So kann z.B. mit zwei 100GB Festplatten ein 200GB logisches Volumen erstellt werden. Oder es kann ein 150GB und ein 50GB logisches Volumen erstellt werden. Eine Kombination von logischen Volumen bis zur Gesamtkapazität (200GB in diesem Beispiel) ist möglich. Die Möglichkeiten sind nur durch die Anforderungen in Ihrem Unternehmen begrenzt.

Dies ermöglicht einem Systemadministrator, jeden Speicher als Teil eines Pools zu betrachten, der in jeglicher Größe zur Verfügung steht. Zusätzlich dazu können Treiber zu diesem Pool hinzugefügt werden, was dies zu einem einfachen Prozess zur vorausschauenden Verwaltung der Speicheranforderungen Ihrer Benutzer werden lässt.

5.6.3.2. Logisches Volumen in der Größe anpassen

Die Eigenschaft, die die meisten Systemadministratoren an LVM schätzen, ist dessen Möglichkeit Speicher einfach dorthin zu lenken, wo dieser gerade am meisten benötigt wird. In einer Nicht-LVM-Systemkonfiguration führt das Vorhandensein von ungenügend Speicherplatz — bestenfalls — zum Verschieben von Dateien auf ein Gerät mit noch freiem Platz. Häufig bedeutet dies eine Neukonfiguration der Massenspeichergeräte Ihres Systems. Eine Aufgabe, die außerhalb der eigentlichen Geschäftszeiten durchgeführt werden muss.

LVM macht es jedoch möglich, auf einfache Weise die Größe eines logischen Volumens zu erhöhen. Nehmen wir an, dass unser 200GB Speicherpool für das Erstellen eines 150GB logischen Volumens verwendet wurde, wobei die restlichen 50GB als Reserve dienen. Ist das 150GB logische Volumen voll, kann über LVM dessen Größe (z.B. um 10 GB) ohne physikalische Neukonfiguration geändert werden. Anhängig von der Systemumgebung kann dies dynamisch geschehen oder eventuell eine kurze Downtime für die eigentliche Größenänderung in Anspruch nehmen.

5.6.3.3. Datenmigration

Die meisten erfahrenen Systemadministratoren wären von den Fähigkeiten von LVM beeindruckt, würden sich aber folgende Fragen stellen:

Was passiert, wenn eine der Festplatten, aus denen ein logisches Volumen besteht, auszufallen beginnt?

Die gute Nachricht ist, dass die meisten LVM-Implementierungen die Fähigkeit haben, Daten von einer bestimmten physikalischen Festplatte zu *migrieren*. Damit dies funktioniert, müssen genügend Ressourcen zur Verfügung stehen, um den Verlust der ausfallenden Festplatte auszugleichen. Sobald die Migration abgeschlossen ist, kann die ausgefallene Festplatte ersetzt und wieder in den Speicherpool eingefügt werden.

5.6.3.4. Mit LVM, warum RAID benutzen?

Da LVM einige Fähigkeiten hat, die RAID ähneln (z.B. die Fähigkeit, dynamisch ausgefallene Festplatten zu ersetzen) und außerdem einige Fähigkeiten besitzt, die von den meisten RAID-Implementationen nicht übertroffen werden können (z.B. die Fähigkeit, dynamisch mehr Speicher zu einem zentralen Speicherpool hinzuzufügen), fragen sich viele ob RAID dann immer noch eine wichtige Rolle spielt.

Nichts liegt der Wahrheit ferner. RAID und LVM sind komplementäre Technologien, die zusammen verwendet werden können (ähnlich wie nested RAID-Level) und es daher ermöglichen, das Beste aus beiden herauszuholen.

5.7. Tagtägliche Speicherverwaltung

Systemadministratoren müssen im Laufe ihrer tagtäglichen Arbeit auf Speicher achten. Es gibt verschiedene Probleme, die dabei bedacht werden müssen:

- Freien Speicherplatz überwachen
- Probleme mit Festplattenquoten
- Datei-bezogene Probleme
- Verzeichnis-bezogene Probleme
- Backup-bezogene Probleme
- Performance-bezogene Probleme
- Speicher hinzufügen/entfernen

Die folgenden Abschnitte beschreiben jedes dieser Probleme in größerem Detail.

5.7.1. Freien Speicher überwachen

Das Sicherstellen, dass genügend freier Speicherplatz zur Verfügung steht, steht täglich ganz oben auf der Liste eines Systemadministrators. Der Grund, warum regelmäßiges, häufiges Überprüfen auf freien Speicherplatz so wichtig ist, ist die Tatsache, dass freier Platz so dynamisch ist; einen Moment lang kann es genug freien Speicher geben und dann im nächsten Moment wiederum fast gar keinen.

Im Allgemeinen gibt es drei Gründe für einen Mangel an freiem Speicherplatz:

- Übermäßige Nutzung durch einen Benutzer
- Übermäßige Nutzung durch eine Applikation

- Normales Ansteigen der Nutzung

Diese Gründe werden in den nächsten Abschnitten genauer beschrieben.

5.7.1.1. Übermäßige Nutzung durch einen Benutzer

Verschiedene Personen haben eine unterschiedliche Auffassung von Ordnungsliebe. Einige sind geschockt, wenn sich ein paar Staubkörnchen auf deren Tisch befinden, während andere eine Kollektion alter Pizzakartons des vergangenen Jahres neben dem Sofa besitzen. Das selbe gilt bei deren Umgang mit Speicher:

- Einige sind sehr genau mit deren Umgang der Speicherverwendung und lassen niemals ungenutzte Dateien irgendwo auf dem System herumliegen.
- Andere scheinen nie die Zeit zu finden, um unnütze Dateien loszuwerden, die nicht mehr länger benötigt werden.

Sind Benutzer für die Verwendung großer Speichermengen verantwortlich, sind dies häufig solche der zweiten Gruppe.

5.7.1.1.1. Der Umgang mit übermäßiger Speichernutzung eines Benutzers

Dies ist ein Bereich, in dem Systemadministratoren alle ihre diplomatischen und sozialen Fähigkeiten einsetzen müssen. Häufig werden Diskussionen über Festplattenplatz emotional, da einige der Benutzer die Einschränkungen der Nutzung der Festplatte als Erschwerung ihrer Arbeit ansehen oder als nicht in diesem Umfang gerechtfertigte Maßnahme oder sie einfach glauben nicht die Zeit zu haben, ihre Dateien aufzuräumen.

Der geübte Systemadministrator berücksichtigt in solchen Situationen viele Faktoren. Sind die Einschränkungen fair und vernünftig für die Art der Arbeit, die von dieser Person ausgeführt wird? Nutzt diese Person ihren Festplattenplatz angemessen? Können Sie dieser Person helfen, die Speichernutzung zu reduzieren (z.B. in dem Sie eine Backup-CD-ROM aller E-Mails des letzten Jahres oder so anlegen)? Ihre Aufgabe während des Gesprächs ist es, genau dies herauszufinden und dabei auch sicherzustellen, dass jemand, der soviel Platz nicht benötigt, aufräumt.

Egal wie, Sie sollten auf jeden Fall das Gespräch auf einer professionellen, faktischen Ebene führen. Versuchen Sie, die Probleme des Benutzers höflich anzusprechen ("Ich verstehe, dass Sie sehr beschäftigt sind, aber Ihre Mitarbeiter in Ihrer Abteilung haben die gleiche Verantwortung, keinen Speicher zu verschwenden und deren durchschnittliche Nutzung liegt bei der Hälfte von dem, was Sie verwenden") und das Gespräch auf das eigentliche Problem lenken. Bieten Sie Hilfe an, wenn das Problem mangelnde Kenntnisse/Erfahrung ist.

Das Angehen an eine Situation auf einfühlsame jedoch bestimmte Art und Weise ist häufig besser als das Einsetzen Ihrer Autorität als Systemadministrator, um ein gewisses Resultat zu erzwingen. Manchmal ist zum Beispiel auch ein Kompromiss zwischen Ihnen und dem Benutzer nötig. Dieser Kompromiss kann eine der drei Formen annehmen:

- Temporären Speicherplatz vergeben
- Archivbackups durchführen
- Aufgeben

Sie werden vielleicht merken, dass Benutzer ihre Speichernutzung einschränken, wenn diese eine gewisse Menge an temporärem Speicherplatz zur Verfügung haben, den sie ohne Einschränkung verwenden können. Dies ermöglicht ihnen, ohne Sorge um den Speicher zu arbeiten, bis ein gewisser Punkt erreicht ist, an dem dann aufgeräumt und somit festgestellt werden kann, welche Dateien im temporären Speicher wirklich benötigt werden und welche nicht.

Achtung

Wenn Sie diese Möglichkeit anbieten, tappen Sie *nicht* in die Falle, diesen temporären Speicherplatz zum permanenten Speicherplatz werden zu lassen. Lassen Sie keine Zweifel offen, dass dieser Speicherplatz nur temporär ist und es keine Garantie gibt, Daten aufzubewahren: es werden keine Backups von Daten im temporären Speicherplatz angefertigt.

Viele Systemadministratoren unterstreichen diese Tatsache, in dem sie automatisch alle Dateien im temporären Speicher löschen, die älter als ein gewisses Datum sind (z.B. nach einer Woche).

Manchmal besitzt ein Benutzer auch viele Dateien, die offensichtlich so alt sind, dass ständiger Zugriff auf diese relativ unwahrscheinlich ist. Stellen Sie sicher, das dies auch der Fall ist. Manchmal sind einzelne Benutzer auch für die Instandhaltung eines Archiv alter Daten zuständig; dann sollten Sie diesen durch die Erstellung mehrerer Backups behilflich sein, die genauso wie die archivischen Backups des Datenzentrums behandelt werden.

Es gibt jedoch auch Umstände, bei denen der Wert der Daten etwas dubios erscheint. Hier ist es hilfreich, ein spezielles Backup anzubieten. Sie führen ein Backup der alten Daten durch und geben dem Benutzer dieses Backup, wobei Sie gleichzeitig erklären, dass der Benutzer für die Aufbewahrung verantwortlich ist. Sollte Zugriff auf die Daten ermöglicht werden, sollte der Benutzer Sie (oder den jeweilig Verantwortlichen — wie auch immer dies in Ihrem Unternehmen gehandhabt wird) bitten, die Daten wiederherzustellen.

Es müssen einige Dinge beachtet werden, damit dies nicht zum Problem wird. Als erstes sollten Sie keine Backups von Dateien durchführen, die wahrscheinlich noch gebraucht werden; wählen Sie keine Dateien, die *viel zu* neu sind. Als nächstes sollten Sie sicherstellen, dass Sie in der Lage sind, die Daten wiederherzustellen, sollte dies gewünscht werden. Dies bedeutet, das die Backup-Medien in einem Format sind, von dem Sie sicher sind, das dieses in der nächsten Zukunft von Ihrem Datenzentrum weiter unterstützt wird.

Tipp

Ihre Wahl des Backup-Mediums sollte auch die Technologien in Betracht ziehen, die den Benutzer die Datenwiederherstellung alleine durchführen lassen können. So ist zum Beispiel das Sichern mehrerer Gigabytes auf CD-R mehr Arbeit als das Speichern auf Band mit einem einzigen Befehl, aber denken Sie daran, dass der Benutzer auf die Daten auf CD-R selbst zugreifen kann, wann auch immer er diese benötigt — ohne dass Sie dabei involviert sein müssen.

5.7.1.2. Übermäßige Nutzung durch eine Applikation

Manchmal sind Applikationen für übermäßige Nutzung verantwortlich. Die Gründe hierfür sind verschieden, können aber folgende enthalten:

- Verbesserungen in der Funktionalität der Applikation erfordern mehr Speicher
- Ein Ansteigen der Benutzerzahl, die diese Applikation verwenden
- Die Applikation räumt nicht auf und lässt nicht länger benötigte, temporäre Dateien auf der Festplatte
- Die Applikation funktioniert nicht richtig, und verwendet mehr Speicher als vorgesehen

Ihre Aufgabe ist es festzulegen, welche der Gründe auf dieser Liste auf Ihre Situation zutreffend sind. Indem Sie die Applikationen sowie das Benutzerverhalten in Ihrem Datencenter kennen, sollten Sie in der Lage sein, einige dieser Gründe auszuschließen. Was danach oft noch zu tun ist, ist ein wenig

detektivische Arbeit, indem nachgeforscht wird, was mit dem Speicher geschehen ist. Dies sollte schlussendlich den Bereich stark eingrenzen.

Sie müssen nun die angemessenen Schritte einleiten; sei es das Hinzufügen von Speicher, um eine beliebte Applikation zu unterstützen, das Kontaktieren der Entwickler dieser Applikation, um Dateicharakteristika zu diskutieren oder das Erstellen von Skripts, um hinter der Applikation aufzuräumen.

5.7.1.3. Normales Ansteigen der Nutzung

Die meisten Unternehmen erfahren langfristig einen gewissen Grad an Wachstum. Daher ist es normal, ein Wachstum der Speichernutzung zu erwarten. In den meisten Situationen kann eine kontinuierliche Überwachung die durchschnittlichen Speichernutzung in Ihrem Unternehmen aufzeigen; diese Rate kann dann verwendet werden, um den Zeitpunkt zu bestimmten, an dem zusätzlicher Speicher hinzugefügt werden sollte, noch bevor Ihr freier Speicherplatz nicht mehr ausreicht.

Wenn Sie aufgrund normalem Wachstums unerwartet nicht mehr genügend Speicherplatz haben sollten, dann haben Sie Ihre Aufgaben nicht richtig erfüllt.

Manchmal können große zusätzliche Anforderungen an den Systemspeicher unerwartet auftreten. Ihr Unternehmen hat vielleicht mit einem anderen Unternehmen fusioniert und erfordert nun schnelle Änderungen in der IT-Infrastruktur (und daher auch in Bezug auf den Speicher). Oder ein neues Projekt mit hoher Priorität ist mehr oder weniger über Nacht hereingekommen. Änderungen an einer bestehenden Applikation könnten ebenso zu generell erhöhtem Speicherbedarf geführt haben.

Egal welches Ereignis dafür verantwortlich ist, es wird immer Zeiten geben, an denen Sie überrumpelt werden. Um sich auf diese Dinge vorzubereiten, sollten Sie die Speicherarchitektur für größte Flexibilität konfigurieren. Speicher in Reserve zu haben (wenn möglich) kann die Auswirkungen solch ungeplanter Vorkommnisse ausgleichen.

5.7.2. Probleme mit Festplattenquoten

Oftmals ist das Erste, das vielen zum Thema Festplattenquote in den Sinn kommt, dass diese dazu verwendet werden, um Benutzer dazu zu zwingen, deren Verzeichnisse aufgeräumt zu halten. Während dies in einigen Fällen zutrifft, hilft es auch gleichzeitig, das Problem der Nutzung von Festplattenplatz von einer anderen Perspektive aus zu betrachten. Was ist zum Beispiel mit Applikationen, die aus verschiedenen Gründen zu viel Speicher benötigen? Es ist schon vorgekommen, dass Applikationen derartig ausfallen, dass sie den gesamten verfügbaren Festplattenplatz einnehmen. In solchen Fällen können Festplattenquoten den Schaden durch solche Applikationen begrenzen und diese zwingen, anzuhalten, *bevor* der gesamte freie Platz verwendet wurde.

Der schwierigste Teil der Implementierung und Verwaltung von Festplattenquoten ist das eigentliche Festlegen der Grenzen. Wie hoch sollen diese sein? Ein einfacher Ansatz wäre, den Festplattenplatz einfach gleichmäßig auf die Benutzer und/oder Gruppen aufzuteilen und diese Zahl dann als Quote pro Benutzer festzulegen. Wenn zum Beispiel ein System eine 100 GB Festplatte und 20 Benutzer hat, sollten jedem Benutzer nicht mehr als 5 GB zugewiesen werden. Auf diese Weise hätte jeder Benutzer 5 GB (die Festplatte wäre dann jedoch zu 100% voll).

Für Betriebssysteme, die dies ermöglichen, können höhere, temporäre Quoten gesetzt werden — zum Beispiel auf 7,5 GB mit einer permanenten Quote von 5 GB. Dies hat den Vorteil, dass Benutzer permanent nur ihre eigene Quote verwenden können, erlaubt jedoch eine gewisse Flexibilität, sollte ein Benutzer diese Grenze erreichen (oder überschreiten). Wenn Sie die Festplattenquote so einsetzen, überbelegen Sie genaugenommen den verfügbaren Festplattenplatz. Die temporäre Quote ist 7,5 GB. Überschreiten alle 20 Benutzer ihre permanente Quote zur gleichen Zeit und versuchen nun, ihre temporäre Quote auszunutzen, müsste die 100GB Festplatte eigentlich 150 GB fassen, damit jeder zur gleichen Zeit die temporäre Quote nutzen kann.

In der Praxis überschreitet aber nicht jeder Benutzer die permanente Quote zur gleichen Zeit, was eine gewisse Überbelegung zu einem vernünftigen Ansatz werden lässt. Die Festlegung der permanenten und temporären Quoten ist dem Systemadministrator überlassen, da jeder Einsatzort und jede Benutzergemeinschaft verschieden sind.

5.7.3. Datei-bezogene Probleme

Systemadministratoren müssen sich häufig mit datei-bezogenen Problemen beschäftigen. Diese Probleme umfassen die folgenden:

- Dateizugang
- Datei-Sharing

5.7.3.1. Dateizugang

Probleme mit dem Dateizugang drehen sich meistens um ein Szenario — ein Benutzer kann nicht auf eine Datei zugreifen, auf welche dieser aber seiner Meinung nach Zugriff haben sollte.

Meistens entsteht dies Problem, wenn Benutzer 1 eine Kopie einer Datei an Benutzer 2 weitergeben möchte. In den meisten Unternehmen sind die Berechtigungen für einen Benutzer, auf die Dateien eines anderen Benutzers zuzugreifen, stark eingeschränkt, was dieses Problem hervorruft.

Es gibt drei Ansätze, die verfolgt werden können:

- Benutzer 1 führt die nötigen Änderungen durch, so dass Benutzer 2 auf die Datei zugreifen kann.
- Ein Bereich für den Datenaustausch wird für solche Zwecke angelegt; Benutzer 1 legt eine Kopie der Datei hier ab, die dann von Benutzer 2 kopiert werden kann.
- Benutzer 1 verwendet E-Mail, um Benutzer 2 eine Kopie der Datei zu übermitteln.

Es gibt allerdings ein Problem mit der ersten Betrachtungsweise — abhängig davon, wie Zugriffsrechte vergeben werden, kann Benutzer 2 auf alle Dateien des Benutzer 1 zugreifen. Schlimmer noch, es kann auch geschehen, dass auf einmal *alle* Benutzer im Unternehmen auf die Dateien von Benutzer 1 zugreifen können. Nochviel schlimmer ist es, wenn diese Änderungen nicht rückgängig gemacht werden können, nachdem Benutzer 2 keinen Zugang mehr benötigt und somit die Dateien von Benutzer 1 permanent allen anderen zugängig sind. Leider ist das Thema Sicherheit, wenn Benutzer die Verantwortlichen in dieser Situation sind, selten eine der höchsten Prioritäten.

Der zweite Ansatz eliminiert das Problem, dass alle Dateien von Benutzer 1 für allen anderen zugänglich sind. Sobald jedoch eine Datei sich im Datenaustauschbereich befindet, kann die Datei von allen anderen gelesen (und abhängig von den Berechtigungen, auch geschrieben) werden. Dieser Ansatz hat desweiteren das Problem, dass der Datenaustauschbereich mit Dateien überfüllt wird, da Benutzer häufig vergessen, ihre Dateien aufzuräumen.

Der dritte Ansatz, wenn dieser auch umständlich klingt, ist wahrscheinlich in den meisten Fällen der Beste. Durch standardmäßige E-Mail-Anhangsprotokolle und intelligentere E-Mailprogramme wird das Senden von Dateien zum Kinderspiel und erfordern keine Einmischung vom Systemadministrator. Es besteht natürlich die Chance, dass jemand eine 1GB-Datenbankdatei an alle 150 Mitarbeiter in der Finanzabteilung verschicken möchte, daher ist ein gewisser Grad an Benutzertraining (und gewisse Grenzen für E-Mail-Anhänge) sinnvoll. Keiner dieser Ansätze behandelt jedoch das Problem, wenn zwei oder mehr Benutzer ständigen Zugang zu einer Datei benötigen. In diesem Fall sind andere Methoden notwendig.

5.7.3.2. Datei-Sharing

Benötigen mehrere Benutzer Zugang zu einer einzigen Datei, ist das Gewähren von Zugang über das Ändern der Zugriffsrechte nicht der beste Ansatz. Es ist auf jeden Fall vorzuziehen, den Status der Datei zu formalisieren. Hierfür gibt es mehrere Gründe:

- Dateien, die über ein Benutzerverzeichnis gemeinsam verwendet werden, sind sehr anfällig dafür, unerwartet zu verschwinden, wenn ein Benutzer zum Beispiel die Firma verlässt oder einfach nur seine Dateien neu ordnet.
- Die Wartung eines Shared-Access für mehr als zwei Benutzer wird schwieriger, was zu einem langfristigen Problem an unnötiger Arbeit wird, wenn die zusammenarbeitenden Benutzer ihren Verantwortungsbereich wechseln.

Hierfür ist einer der besten Ansätze:

- Die Benutzer sollten die direkten Besitzerrechte der Datei aufgeben
- Eine Gruppe erstellen, die diese Datei besitzt
- Die Datei in einem gemeinsam verwendeten Verzeichnis ablegen, das der Gruppe gehört
- Alle Benutzer, die Zugang zu dieser Datei brauchen, als Teil der Gruppe anlegen

Dieser Ansatz funktioniert auch mit mehreren Dateien und kann verwendet werden, um Speicher für große, komplexe Projekte zuzuweisen.

5.7.4. Speicher hinzufügen/löschen

Da der Bedarf an zusätzlichem Festplattenplatz nie endet, muss ein Systemadministrator häufig neuen Festplattenplatz hinzufügen oder manchmal ältere, kleinere Festplatten entfernen. In diesem Abschnitt erhalten Sie Informationen zum Hinzufügen und Entfernen von Speicher.

Anmerkung

Auf vielen Betriebssystemen werden Massenspeichergeräte nach ihrer physikalischen Verbindung zum System benannt. Daher kann das Hinzufügen oder Entfernen von Massenspeichergeräten zu Änderungen in den Gerätenamen führen. Wenn Sie Speicher hinzufügen oder entfernen, sollten Sie grundsätzlich sicherstellen, dass alle Referenzen zu Gerätenamen, die von Ihrem Betriebssystem verwendet werden, akutell sind.

5.7.4.1. Speicher hinzufügen

Der Vorgang des Hinzufügens von Speicher zu einem Computersystem ist relativ einfach. Hier die grundlegenden Schritte:

1. Hardware installieren
2. Partitionieren
3. Partitionen formatieren
4. Systemkonfiguration aktualisieren
5. Backup-Planung ändern

Die folgenden Abschnitte beschreiben jeden dieser Schritte eingehender.

5.7.4.1.1. Hardware installieren

Bevor irgendetwas anderes gemacht werden kann, muss die neue Festplatte installiert und zugänglich gemacht werden. Während es viele verschiedene mögliche Konfigurationen gibt, beschreiben die folgenden Abschnitte die beiden häufigsten Arten — das Hinzufügen einer ATA- oder einer SCSI-Festplatte. Die hier aufgeführten grundlegenden Schritte sind auch auf andere Konfigurationen anwendbar.

Tipp

Egal welche Speicher-Hardware Sie verwenden, Sie sollten immer die zusätzliche Last einer neuen Festplatte für das I/O-Subsystem Ihres Computers beachten. Im Allgemeinen sollten Sie versuchen, die I/O Last über alle Kanäle/Busse zu verteilen. Vom Performance-Standpunkt aus ist es wesentlich besser, alle Festplatten auf einen Kanal zu legen und den anderen Kanal leer zu lassen.

5.7.4.1.1.1. ATA Festplatten hinzufügen

ATA Festplatten werden häufig in Desktop- und kleineren Serversystemen eingesetzt. Fast alle Systeme in diesen Kategorien besitzen integrierte ATA-Controller mit mehreren ATA-Kanälen — meistens zwei bis vier.

Jeder Kanal kann zwei Geräte unterstützen — "Master" und "Slave". Diese beiden Geräte sind über ein Kabel mit dem Kanal verbunden. Aus diesem Grund ist dabei der erste Schritt festzustellen, welche Kanäle verfügbaren Platz für eine zusätzliche Festplatte haben. Eine der folgenden drei Situationen ist möglich:

- Es gibt einen Kanal mit nur einer verbundenen Festplatte
- Es gibt einen Kanal ohne angeschlossene Festplatte
- Es ist kein freier Platz vorhanden

Die erste Situation ist meistens die einfachste, da es wahrscheinlich ist, dass das Kabel einen unbenutzten Stecker hat, an den die neue Festplatte angeschlossen werden kann. Hat das Kabel jedoch nur zwei Stecker (einen für den Kanal und den anderen für die bereits installierte Festplatte) dann müssen Sie dieses Kabel durch eines mit drei Steckern ersetzen.

Bevor Sie die neue Festplatte installieren, stellen Sie sicher, dass die Festplatten, die sich den Kanal teilen, richtig konfiguriert sind (eine als Master, eine als Slave).

Die zweite Situation ist etwas schwieriger, aber nur insofern, dass Sie ein Kabel beschaffen müssen, sodass Sie eine Festplatte an den Kanal anschließen können. Die neue Festplatte kann als Master oder Slave konfiguriert werden (traditionell ist die erste Festplatte auf einem Kanal ein Master).

In der dritten Situation gibt es keinen freien Platz für eine zusätzliche Festplatte. Sie müssen nun eine Entscheidung treffen. Sie können:

- Eine ATA-Controller-Karte beschaffen und diese installieren
- Eine der bestehenden Festplatten durch eine neue, größere Festplatte ersetzen

Das Hinzufügen einer Controller-Card umfasst das Prüfen der Hardware-Kompatibilität, physikalische Kapazität und Software-Kompatibilität. Die Karte muss mit den Bus-Slots des Computers kompatibel sein, es muss ein freier Slot bestehen und sie muss von Ihrem Betriebssystem unterstützt werden. Das Ersetzen einer installierten Festplatte konfrontiert Sie jedoch mit einem einzigartigen Problem: was passiert mit den Daten auf dieser Festplatte? Hierfür gibt es einige Möglichkeiten:

- Schreiben Sie die Daten auf ein Backup-Gerät und stellen Sie diese nach der Installation der neuen Festplatte wieder her
- Nutzen Sie Ihr Netzwerk, um die Daten auf ein anderes System mit genügend freiem Speicherplatz zu kopieren und stellen Sie die Daten nach der Installation der neuen Festplatte wieder her
- Verwenden Sie den Speicherplatz, der von einer dritten Festplatte physikalisch verwendet wird, indem Sie:
    1. Die dritte Festplatte temporär entfernen
    2. Die neue Festplatte temporär an deren Stelle installieren
    3. Die Daten auf die neue Festplatte kopieren
    4. Die alte Festplatte entfernen
    5. Die alte durch die neue Festplatte ersetzen
    6. Die temporär entfernte dritte Festplatte neu installieren

- Die eigentliche Festplatte und die neue Festplatte temporär auf einem anderen Computer installieren, die Daten auf die neue Festplatte kopieren und die neue Festplatte dann im ursprünglichen Computer installieren

Wie Sie sehen, müssen Sie einige Mühe aufwenden, um die Daten (und die neue Hardware) wieder an Ort und Stelle zu bekommen.

5.7.4.1.1.2. Hinzufügen von SCSI-Festplatten

SCSI-Festplatten werden gewöhnlich in größeren Workstations und Serversystemen eingesetzt. Im Gegensatz zu ATA-basierten Systemen können SCSI-Systeme integrierte SCSI-Controller besitzen oder auch nicht; wohingegen andere auch eine separate SCSI-Controller-Karte verwenden.

Die Fähigkeiten der SCSI-Controller (eingebaut oder extern) unterscheiden sich auch weitläufig. Sie bieten entweder einen engen oder weiten SCSI-Bus. Die Bus-Geschwindigkeit beträgt entweder Normal, Fast, Ultra, Ultra2 oder Ultra160.

Falls Sie mit diesen Begriffen nicht vertraut sind (diese wurden kurz im Kapitel Abschnitt 5.3.2.2 beschrieben), müssen Sie die Fähigkeiten Ihrer Hardwarekonfiguration feststellen und eine passendes neues Laufwerk wählen. Die beste Quelle für Informationen hierzu ist die Dokumentation zu Ihrem System und/oder dem SCSI-Adapter.

Sie müssen dann herausfinden, wieviele SCSI-Busse auf Ihrem System zur Verfügung stehen und welche davon Platz für eine neue Festplatte haben. Die Anzahl der SCSI-unterstützten Geräte hängt von der Busbreite ab:

- Narrow (8-Bit) SCSI-Bus — 7 Geräte (plus Controller)
- Wide (16-Bit) SCSI-Bus — 15 Geräte (plus Controller)

Der erste Schritt dabei ist festzustellen, welche Busse freien Platz für eine zusätzliche Festplatte haben. Sie finden dabei eine der drei folgenden Situationen vor:

- Es gibt einen Bus, an den weniger als die maximale Anzahl von Festplatten angeschlossen ist
- Es gibt einen Bus, an den keine Festplatten angeschlossen sind
- Es gibt auf keinem Bus freien Platz

Die erste Situation ist meistens die Einfachste, da das Kabel wahrscheinlich einen unbenutzten Stecker hat, an den die neue Festplatte angeschlossen werden kann. Hat das Kabel jedoch keinen freien Stecker, müssen Sie das Kabel durch eines ersetzen, das mindestens einen Stecker mehr hat.

Die zweite Situation ist etwas schwieriger, wenn auch nur daher, dass Sie irgendwie ein Kabel beschaffen müssen, mit dem Sie die Festplatte an den Bus anschließen können.

Wenn es nicht genügend Platz für eine zusätzliche Festplatte gibt, müssen Sie eine Entscheidung treffen. Möchten Sie:

- Eine SCSI-Controller-Karte beschaffen und diese installieren
- Eine der installierten Festplatten durch eine neue, größere Festplatte ersetzen

Das Hinzufügen einer Controller-Card bringt das Prüfen auf Hardware-Kompatibilität, physikalischer Kapazität und Software-Kompatibilität mit sich. Die Karte muss mit den Bus-Slots des Computers kompatibel sein. Es muss ein freier Slot bestehen und die Karte muss von Ihrem Betriebssystem unterstützt werden.

Das Ersetzen einer installierten Festplatte bereitet ein einzigartiges Problem: was passiert mit den Daten auf dieser Festplatte? Hierfür gibt es einge Möglichkeiten:

- Schreiben Sie die Daten auf ein Backup-Gerät und stellen Sie diese nach der Installation der neuen Festplatte wieder her
- Nutzen Sie Ihr Netzwerk, um die Daten auf ein anderes System mit genügend freiem Speicherplatz zu kopieren und stellen Sie die Daten nach der Installation der neuen Festplatte wieder her
- Verwenden Sie den Speicherplatz, der von einer dritten Festplatte physikalisch verwendet wird, indem Sie:
    1. Die dritte Festplatte temporär entfernen
    2. Die neue Festplatte temporär an deren Stelle installieren
    3. Die Daten auf die neue Festplatte kopieren
    4. Die alte Festplatte entfernen
    5. Die alte durch die neue Festplatte ersetzen
    6. Die temporär entfernte dritte Festplatte neu installieren

- Die eigentliche Festplatte und die neue Festplatte temporär auf einem anderen Computer installieren, die Daten auf die neue Festplatte kopieren und die neue Festplatte dann im ursprünglichen Computer installieren

Sobald Sie einen Stecker zur Verfügung haben, an den Sie die neue Festplatte anschließen können, müssen Sie sicherstellen, dass die SCSI-ID der Festplatte richtig gesetzt ist. Hierfür müssen Sie wissen, welche IDs alle anderen Geräte am Bus (inklusive Controller) für ihre SCSI verwenden. Am einfachsten finden Sie dies heraus, wenn Sie auf das BIOS des SCSI-Controllers zugreifen. Dies geschieht gewöhnlich durch das Drücken einer bestimmten Tastenfolge während des Booten des Systems. Sie können sich dann die Konfiguration des SCSI-Controllers und aller Geräte, die an allen Bussen angeschlossen sind, ansehen.

Als nächstes müssen Sie den richtigen Abschluss des Busses beachten. Wenn Sie eine neue Festplatte hinzufügen, sind die Regeln ziemlich einfach — wenn die neue Festplatte das letzte (oder einzige) Gerät auf dem Bus ist, muss diese einen Endwiderstand haben. Ansonsten muss der Endwiderstand aktiviert sein.

Jetzt können Sie zum nächsten Schritt im Prozess übergehen — das Partitionieren Ihrer neuen Festplatte.

5.7.4.1.2. Partitionieren

Sobald die Festplatte installiert ist, können Sie eine oder mehr Partitionen erstellen, um den Speicherplatz für Ihr Betriebssystem zur Verfügung zu stellen. Die Tools hierfür variieren von Betriebssystem zu Betriebssystem, aber die grundlegenden Schritte bleiben die gleichen:

1. Wählen Sie die neue Festplatte aus
2. Sehen Sie sich die aktuelle Partitionstabelle der Festplatte an, um sicherzustellen, dass die Festplatte, die Sie partitionieren wollen, auch wirklich die Richtige ist
3. Löschen Sie alle unerwünschten Partitionen, die sich eventuell noch auf der neuen Festplatte befinden
4. Erstellen Sie die neuen Partitionen und stellen Sie sicher, dass Sie die gewünschte Größe und den Partitionstyp angeben
5. Speichern Sie die Änderungen und verlassen Sie das Partitionsprogramm

Achtung

Bei der Partitionierung einer neuen Festplatte ist es *wichtig*, dass Sie sicher sind, das Sie die richtige Festplatte partitionieren. Ansonsten laufen Sie Gefahr, eine Festplatte zu partitionieren, die bereits verwendet wird, was in Datenverlust endet.

Stellen Sie auch sicher, dass Sie die beste Partitionsgröße gewählt haben. Überlegen Sie sich dies gut, denn ein nachträgliches Ändern ist wesentlich schwieriger als sich jetzt ein bisschen Zeit zu nehmen um dies zu durchdenken.

5.7.4.1.3. Partitionen formatieren

Jetzt besitzt die neue Festplatte eine oder mehr Partitionen. Bevor jedoch der Speicherplatz auf diesen Partitionen verwendet werden kann, müssen diese erst formatiert werden. Durch das Formatieren wählen Sie ein bestimmtes Dateisystem aus, das mit jeder Partition verwendet werden soll. Dies ist ein wichtiger Punkt im Leben dieser Festplatte; die Entscheidungen, die Sie hier treffen können später nicht ohne großen Aufwand rückgängig gemacht werden.

Das eigentliche Formatieren geschieht über ein Utility-Programm; die jeweilig durchzuführenden Schritte hängen vom Betriebssystem ab. Sobald die Formatierung abgeschlossen ist, ist die Festplatte richtig für den Einsatz konfiguriert.

Bevor Sie fortfahren, sollten Sie Ihre Arbeit prüfen, indem Sie auf die Partition zugreifen und sicherstellen, dass alles in Ordnung ist.

5.7.4.1.4. Systemkonfiguration aktualisieren

Sollte Ihr Betriebssystem jegliche Konfigurationsänderungen zur Verwendung des neuen Speichers benötigen, ist jetzt der Zeitpunkt, diese Änderungen durchzuführen.

Sie können relativ sicher sein, dass das Betriebssystem ordnungsgemäß konfiguriert ist, um den neuen Speicher automatisch zugänglich zu machen, wenn das System bootet (wenn Sie die Zeit haben, Ihr System schnell einmal neu hochzufahren, ist dies sicherlich sinnvoll — nur um sicherzugehen).

Im nächsten Abschnitt erfahren Sie mehr über einige häufig vergessene Schritte beim Hinzufügen von neuem Speicher.

5.7.4.1.5. Ändern der Backup-Planung

Davon ausgehend, dass der neue Speicher nicht nur temporär ist und keine Backups benötigt, ist dies der Zeitpunkt, die nötigen Änderungen an den Backup-Prozessen durchzuführen, sodass ein Backup des neuen Speichers durchgeführt wird. Die genaue Prozedur hängt davon ab, wie Backups auf Ihrem System durchgeführt werden. Hier finden Sie jedoch einige Punkte, die Sie dabei Auge behalten sollten:

- Überlegen Sie die optimale Backup-Häufigkeit
- Entscheiden Sie, welche Art Backup am angemessensten ist (nur vollständige Backups, vollständig inkrementelle Backups, vollständig differentiale Backups etc)
- Bedenken die Auswirkungen des zusätzlichen Speichers auf die Belegung der Backup-Medien
- Beurteilen Sie, ob die zusätzlichen Backups Auswirkungen auf die anderen Backups haben und versuchen Sie, Zeit außerhalb der eigentlichen Backup-Zeiten hierfür aufzuwenden
- Stellen Sie sicher, dass die Änderungen an die jeweilig betroffenen Personen weitergegeben werden (andere Systemadministratoren, Betriebspersonal etc.)

Sobald Sie all dies durchgeführt haben, können Sie den neuen Speicher verwenden.

5.7.4.2. Speicher entfernen

Das Entfernen von Festplattenplatz von einem System ist einfach, da die meisten Schritte wie in der Installationsabfolge ausgeführt werden (natürlich in umgekehrter Reihenfolge):

1. Verschieben Sie alle zu speichernden Daten von der Festplatte
2. Ändern Sie die Backup-Planung, so dass nicht länger ein Backup dieser Festplatte durchgeführt wird
3. Aktualisieren Sie die Systemkonfiguration
4. Löschen Sie den Inhalt der Festplatte
5. Entfernen Sie die Festplatte

Wie Sie sehen, müssen Sie im Vergleich zum Installationsprozess einige Extra-Schritte durchführen. Diese Schritte werden in den folgenden Abschnitten beschrieben.

5.7.4.2.1. Daten von der Festplatte verschieben

Sollten sich Daten auf der Festplatte befinden, die gespeichert werden müssen, müssen Sie als erstes festlegen, wo die Daten abgelegt werden sollen. Dies hängt im Wesentlichen davon ab, was mit den Daten passieren soll. Wenn die Daten z.B. nicht länger aktiv verwendet werden sollen, sollten diese archiviert werden. Am besten geschieht dies in Form allgemeiner System-Backups. Das bedeutet, dass Sie sich angemessene Aufbewahrungszeiten für dieses endgültige Backup überlegen müssen.

Tipp

Denken Sie daran, dass zusätzlich zu den Datenaufbewahrungrichtlinien Ihres Unternehmens eventuell gesetzliche Regelungen für die Datenaufbewahrung gelten. Kontaktieren Sie daher die jeweilig für die Daten verantwortliche Abteilung, da diese die angemessene Aufbewahrungszeit kennen sollten.

Wenn auf der anderen Seite diese Daten noch genutzt werden, sollten diese auf einem System, das am besten für die Verwendung geeignet ist, abgelegt werden. Ist dies der Fall, wäre es wohl am einfachsten, die Daten zu verschieben, indem Sie die Festplatte auf dem neuen System neu installieren. Wollen Sie dies durchführen, sollten Sie ein vollständiges Backup der Daten anlegen — es wurden schon Festplatten mit wertvollen Daten fallengelassen (und damit alle Daten vernichtet), wobei nichts Gefährlicheres damit gemacht wurde, als damit durch ein Datenzentrum zu laufen.

5.7.4.2.2. Inhalte der Festplatte löschen

Egal ob die Festplatte wertvolle Daten enthielt, ist es auf jeden Fall eine gute Idee, den Inhalt der Festplatte zu löschen, bevor Sie diese anderweitig zuweisen oder aufgeben. Der offensichtliche Grund ist, um sicherzustellen, dass keine empfindlichen Daten auf der Festplatte bleiben. Es ist außerdem ein guter Zeitpunkt, den Zustand der Festplatte zu prüfen, indem Sie einen Lese/Schreib-Test für defekte Blöcke auf dem gesamten Laufwerk durchführen.

Wichtig

Viele Unternehmen (und Behörden) haben spezielle Methoden für das Löschen von Daten auf Festplatten und anderen Speichermedien. Sie sollten *immer* sicherstellen, dass Sie diese Anforderungen verstehen und diese befolgen. In vielen Fällen gibt es rechtliche Auswirkungen, wenn Sie dies nicht tun. Das obige Beispiel sollten keinesfalls als die einzige Methode zum Löschen einer Festplatte betrachtet werden.

Zusätzlich dazu können Unternehmen, die mit empfindlichen Daten arbeiten bestimmten rechtlichen Prozeduren für das Entsorgen von Festplatten unterliegen (zum Beispiel die vollständige Zerstörung dieser). In diesen Fällen sollten Sie sich an die Sicherheitsabteilung für weitere Informationen und Richtlinien wenden.

5.8. Weiteres zu Backups...

Einer der wichtigsten Faktoren bei der Betrachtung von Speicher sind Backups. Wir betrachten dieses Thema hier nicht weiter, da diesem ein ausführlicher Abschnitt (Abschnitt 8.2) gewidmet ist.

5.9. Red Hat Enterprise Linux-spezifische Informationen

Abhängig von Ihrer bisherigen Erfahrung als Systemadministrator ist Ihnen das Verwalten von Speicher unter Red Hat Enterprise Linux entweder weitgehend bekannt oder vollständig unbekannt. Dieser Abschnitt beschreibt Red Hat Enterprise Linux-spezifische Aspekte der Speicherverwaltung.

5.9.1. Gerätenamen-Konventionen

Wie bei allen Linux-ähnlichen Betriebssystemen verwendet Red Hat Enterprise Linux Gerätedateien zum Zugriff auf die gesamte Hardware (inklusive Festplatten). Namenskonventionen für angehängte Speichergeräte variieren jedoch zwischen den verschiedenen Linux- und Linux-ähnlichen Systemen. Im folgenden werden die Benennungen für Gerätedateien unter Red Hat Enterprise Linux beschrieben.

Anmerkung

Gerätenamen unter Red Hat Enterprise Linux werden zum Bootzeitpunkt festgelegt.

Aus diesem Grund können Änderungen an der Systemhardware in einer Änderung der Gerätenamen resultieren, wenn das System neu bootet. Hierdurch können Probleme entstehen, wenn Referenzen zu Gerätenamen in der Systemkonfiguration nicht angemessen aktualisiert werden.

5.9.1.1. Gerätedateien

Unter Red Hat Enterprise Linux erscheinen die Gerätedateien für Festplatten im Verzeichnis `/dev/`. Das Format für jeden Dateinamen hängt von mehreren Aspekten der eigentlichen Hardware und deren Konfiguration ab. Die wichtigsten Punkte sind folgende:

- Gerätetyp
- Unit
- Partition

5.9.1.1.1. Gerätetyp

Die ersten beiden Buchstaben der Gerätedatei beziehen sich auf den speziellen Typ des Geräts. Bei Festplatten gibt es zwei Gerätetypen, die am häufigsten verwendet werden:

- `sd` — Das Gerät ist SCSI-basiert
- `hd` — Das Gerät ist ATA-basiert

Weitere Informationen zu ATA und SCSI finden Sie unter Abschnitt 5.3.2.

5.9.1.1.2. Unit

Die zwei Buchstaben für den Gerätetyp werden gefolgt von einem oder zwei Buchstaben für die jeweilige Unit. Diese Unit-Kennung beginnt mit "a" für die erste Unit, "b" für die zweite und so weiter. Die erste Festplatte auf Ihrem System erscheint daher z.B. als `hda` oder `sda`.

Tipp

Die Fähigkeit von SCSI, eine große Zahl von Geräten anzusprechen erfordert zusätzlich einen zweites Unit-Kennzeichen, um Systeme zu unterstützen, die mehr als 26 SCSI-Geräte besitzen. Die ersten 26 SCSI-Festplatten würden daher `sda` bis `sdz` benannt und die nächsten 26 dann `sdaa` bis `sdaz`.

5.9.1.1.3. Partition

Der letzte Teil des Gerätedateinamens ist eine Ziffer, die eine bestimmte Partition auf dem Gerät angibt, beginnend mit "1". Diese Zahl kann eine oder zwei Ziffern haben, abhängig von der Anzahl der Partitionen auf diesem Gerät. Wenn Sie das Format für die Gerätedateinamen kennen, ist es leicht zu verstehen, worauf diese sich beziehen. Hier einige Beispiele:

- `/dev/hda1` — Die erste Partition auf dem ersten ATA-Laufwerk

- `/dev/sdb12` — Die zwölfte Partition auf dem zweiten SCSI-Laufwerk
- `/dev/sdad4` — Die vierte Partition auf dem dreißigsten SCSI-Laufwerk

5.9.1.1.4. Zugriff zum Gesamt-Gerät

Es kann vorkommen, dass Sie auf das gesamte Laufwerk zugreifen müssen und nicht nur auf eine bestimmte Partition. Dies geschieht normalerweise, wenn das Laufwerk nicht partitioniert ist oder keine Standard-Partitionen unterstützt (wie zum Beispiel ein CD-ROM-Laufwerk). In diesen Fällen wird die Partitionsnummer weggelassen:

- `/dev/hdc` — Das gesamte dritte ATA-Gerät
- `/dev/sdb` — Das gesamte zweite SCSI-Gerät

Die meisten Festplatten verwenden jedoch Partitionen (weitere Informationen zur Partitionierung unter Red Hat Enterprise Linux finden Sie unter Abschnitt 5.9.6.1).

5.9.1.2. Alternativen zu Gerätedateinamen

Da das Hinzufügen oder Entfernen von Massenspeichergeräten in Änderungen an den Gerätedateinamen für bestehende Geräte resultieren kann, besteht das Risiko, dass der Speicher nicht zur Verfügung steht, wenn das System neu startet. Hier ist ein Beispiel einer Abfolge von Ereignissen, die zu diesem Problem führen:

1. Der Systemadministrator fügt einen neuen SCSI-Controller hinzu, sodass zwei neue SCSI-Festplatten an das System angeschlossen werden können (der bestehende SCSI-Bus ist bereits voll)
2. Die ursprünglichen SCSI-Festplatten (inklusive der ersten Festplatte auf dem Bus: `/dev/sda`) werden nicht geändert
3. Das System wir neu gebootet
4. Die SCSI-Festplatte, die bisher als `/dev/sda` bekannt war, hat nun einen neuen Namen, da die erste SCSI-Festplatte auf dem neuen Controller jetzt `/dev/sda` ist

Theoretisch hört sich dies nach einem großen Problem an. Praktisch gesehen ist es dies jedoch aus folgenden Gründen nur selten ein Problem. Als erstes werden Hardware-Konfigurationen dieses Typs nur selten durchgeführt. Zweitens ist es wahrscheinlich, dass der Systemadministrator Downtime geplant hat, um die nötigen Änderungen durchzuführen. Diese benötigen sorgfältige Planung, um sicherzustellen, dass die durchzuführenden Arbeiten nicht länger als die zugewiesene Zeit benötigen. Die Planung hat den positiven Nebeneffekt, dass jegliche Probleme mit den Gerätenamensänderungen ans Licht gebracht werden.

Einige Unternehmen und Systemkonfigurationen werden diesem Problem eventuell begegnen. Unternehmen, die häufig Neukonfigurationen des Speichers benötigen, um deren Anforderungen an Hardware zu erfüllen, verwenden häufig Hardward, die ohne Downtime rekonfiguriert werden kann. Derartige *hotpluggable* Hardware erleichtert das Hinzufügen oder Löschen von Speicher. Unter diesen Umständen kann jedoch das Benennen von Geräten zu einem Problem werden. Glücklicherweise enthält Red Hat Enterprise Linux jedoch Features, die das Ändern von Gerätenamen zu einem kleineren Problem werden lassen.

5.9.1.2.1. Dateisystemkennungen

Einige Dateisysteme (die im Abschnitt Abschnitt 5.9.2 genauer behandelt werden), haben die Möglichkeit, ein *Label (Kennung)* zu speichern — eine Zeichenkette, die die Daten, die das Dateisystem enthält, eindeutig identifiziert. Diese Kennungen können beim Mounten des Dateisystems verwendet werden, was die Verwendung des Gerätenamens umgeht.

Dateisystem-Kennungen funktionieren sehr gut; diese Kennungen müssen jedoch über das gesamte System eindeutig sein. Gibt es mehr als ein Dateisystem mit dem gleichen Label, können Sie unter Umständen nicht auf das Dateisystem zugreifen. Beachten Sie auch, dass Systemkonfigurationen, die keine Dateisysteme verwenden (z.B. einige Datenbanken) nicht die Vorteile von Dateisystemkennungen in Anspruch nehmen können.

5.9.1.2.2. Verwenden von `devlabel`

Die `devlabel`-Software versucht das Gerätenamenproblem anders als Dateisystemkennungen anzusprechen. Die `devlabel`-Software wird von Red Hat Enterprise Linux ausgeführt, wenn das System neu bootet (und wann immer hotpluggable Geräte angeschlossen oder entfernt werden).

Wenn `devlabel` ausgeführt wird, liest es die Konfigurationsdatei (`/etc/sysconfig/devlabel`), um eine Liste der dafür zuständigen Geräte zu erhalten. Für jedes Gerät auf der Liste gibt es einen symbolischen Link (vom Systemadministrator gewählt) und den UUID des Geräts (Universal Unique IDentifier).

Der `devlabel`-Befehl stellt sicher, dass der symbolische Link immer auf das ursprünglich angegebene Gerät weist — auch wenn sich der Gerätename geändert hat. So kann ein Systemadministrator ein System konfigurieren, das z.B. auf `/dev/projdisk` anstelle von `/dev/sda12` weist.

Da die UUID direkt vom Gerät erhalten wird, kann `devlabel` das System nur auf passende UUID durchsuchen und den symbolischen Link anpassen.

Weitere Informationen zu `devlabel` finden Sie im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

5.9.2. Grundlagen zum Dateisystem

Red Hat Enterprise Linux umfasst Support für viele bekannte Dateisysteme, was den Zugriff auf Dateisysteme unter anderen Betriebssystemen erleichtert.

Dies ist insbesondere nützlich für Dual-Boot-Szenarien und wenn Dateien von einem Betriebssystem zu einem anderen migriert werden sollen.

Die unterstützten Dateisysteme umfassen folgende (diese Liste ist nicht vollständig):

- EXT2
- EXT3
- NFS
- ISO 9660
- MSDOS
- VFAT

In den folgenden Abschnitten werden diese Dateisysteme in größerem Detail beschrieben.

5.9.2.1. EXT2

Bis vor Kurzem war das ext2-Dateisystem der Standard für Linux. Als solches hat es umfassendes Testing erfahren und wird als eines der robusteren Dateisysteme angesehen.

Ein perfektes Dateisystem gibt es jedoch nicht, und ext2 stellt hier keine Ausnahme dar. Ein häufig berichtetes Problem ist, dass ext2 einer langwierigen Integritätsprüfung unterzogen werden muss, wenn das System nicht ordnungsgemäß heruntergefahren wurde. Während dies nicht nur auf ext2 zutrifft, bedeutete jedoch die Beliebtheit von ext2 in Verbindung mit größeren Festplatten, dass diese Checks immer länger und länger andauerten. Da musste etwas geschehen.

Im nächsten Abschnitt werden die Ansätze zur Problemlösung unter Red Hat Enterprise Linux beschrieben.

5.9.2.2. EXT3

Das ext3-Dateisystem baut auf ext2 auf, indem Journaling-Fähigkeiten zur bereits bewährten ext2-Codebase hinzugefügt wurden. Als Journaling-Dateisystem eliminiert ext3 den Bedarf an langwierigen Dateisystemprüfungen.

Dies geschieht, indem alle Änderungen am Dateisystem in einem Journal auf der Festplatte verzeichnet werden, was dann regelmäßig geflusht wird. Nach einem unvorhergesehenen Systemvorfall (wie einem Stromausfall oder Systemabsturz) müssen nur die Inhalte des Journals verarbeitet werden, bevor das Dateisystem verfügbar gemacht wird; in den meisten Fällen dauert dies circa eine Sekunde.

Da das Datenformat von ext3 auf ext2 basiert, ist es möglich, auf ein ext3-System von jedem System aus zuzugreifen, das ein ext2-System lesen bzw. schreiben kann (ohne Journaling). Dies kann ein großer Vorteil für Unternehmen sein, in denen einige Systeme ext3 und andere wiederum ext2 verwenden.

5.9.2.3. ISO 9660

In 1987 gab die "International Organization for Standardization" (bekannt als ISO) die Norm 9660 heraus. ISO 9660 legt fest, wie Dateien auf CD-ROMs dargestellt werden. Red Hat Enterprise Linux Systemadministratoren sehen höchstwahrscheinlich ISO 9660 formatierte Daten wahrscheinlich an zwei Orten:

- CD-ROMs
- Dateien (häufig als *ISO-Images* bezeichnet), die vollständige ISO 9660-Dateisysteme enthalten, die auf CD-R oder CD-RW geschrieben werden sollen

Der grundlegende ISO 9660-Standard ist in seiner Funktionalität eher begrenzt, insbesondere im Vergleich zu moderneren Dateisystemen. Dateinamen dürfen maximal 8 Zeichen lang sein und eine Erweiterung von nicht mehr als drei Zeichen haben. Es wurden jedoch verschiedene Erweiterungen zu diesem Standard in den letzten Jahren immer beliebter, unter anderem:

- Rock Ridge — Verwendet einige Felder, die nicht in ISO 9660 definiert sind, um Support für Features wie lange, gemischte Dateinamen, symbolische Links und vernestete Verzeichnisse (mit anderen Worten Verzeichnisse, die wiederum andere Verzeichnisse enthalten) bieten
- Joliet — Eine Erweiterung der ISO 9660-Norm, entwickelt von Microsoft um CD-ROMs ermöglichen zu können, lange Dateinamen mit Hilfe des Unicode-Zeichensatzes zu verwenden

Red Hat Enterprise Linux kann ISO 9660-Dateisysteme, die Rock Ridge und Joliet verwenden, korrekt interpretieren.

5.9.2.4. MSDOS

Red Hat Enterprise Linux unterstützt auch Dateisysteme anderer Betriebssysteme. Wie der Name des msdos-Dateisystems impliziert, war das ursprüngliche Betriebssystem, das diese Dateisystem unterstützt, Microsofts MS-DOS®. Wie in MS-DOS ist ein Red Hat Enterprise Linux-System, das auf ein msdos-Dateisystem zugreift, auf 8.3 Dateinamen beschränkt. Andere Dateiattribute wie Berechtigungen und Besitzer können nicht geändert werden. Vom Standpunkt des Dateiaustausches reicht jedoch das msdos-Dateisystem aus, um die Arbeit zu erledigen.

5.9.2.5. VFAT

Das vfat-Dateisystem wurde zuerst von Microsoft Betriebssystem Windows® 95 verwendet. Als eine Verbesserung des msdos-Dateisystems können Dateinamen auf vfat länger sein als die 8.3 von msdos. Berechtigungen sowie Besitzer können jedoch weiterhin nicht geändert werden.

5.9.3. Dateisysteme mounten

Um auf ein Dateisystem zuzugreifen, muss dies erst *gemountet* werden. In dem Sie ein Dateisystem mounten, weisen Sie Red Hat Enterprise Linux an, eine bestimmte Partition (auf einem bestimmten Gerät) dem System zur Verfügung zu stellen. Wird der Zugriff zu diesem Dateisystem nicht länger benötigt, müssen Sie dieses *unmounten*.

Um ein Dateisystem zu mounten, müssen zwei Informationen gegeben werden:

- Eine Methode, die gewünschte Festplatte und Partition eindeutig zu identifizieren, wie zum Beispiel ein Gerätedateiname, Dateisystemkennung oder ein von `devlabel` verwalteter symbolischer Link
- Ein Verzeichnis, unter dem das gemountete Dateisystem verfügbar gemacht wird (auch bekannt als *Mount-Punkt*)

Im folgenden Abschnitt werden Mount-Punkte weitergehend beschrieben.

5.9.3.1. Mount-Punkte

Wenn Sie noch nicht mit Linux (oder Linux-ähnlichen) Betriebssystemen vertraut sind, erscheint das Konzept der Mount-Punkte eventuell ungewöhnlich. Es ist jedoch eine der leistungsstärksten und flexibelsten Methoden für das Verwalten von Dateisystemen. Bei vielen anderen Betriebssystemen enthält eine vollständige Dateispezifikation den Dateinamen, eine Methode zur genauen Angabe des bestimmten Verzeichnisses in dem sich die Datei befindet und eine Methode zur Identifikation des Geräts auf dem die Datei gefunden werden kann.

Red Hat Enterprise Linux verwendet einen leicht abgeänderten Ansatz. Wie bei anderen Betriebssystemen auch beinhaltet eine vollständige Spezifikation den Dateinamen und das Verzeichnis, in welchem sich die Datei befindet. Es gibt jedoch keine eindeutige Geräteangabe.

Der Grund hierfür ist der Mount-Punkt. Auf anderen Betriebssystemen gibt es eine Verzeichnishierarchie für jede Partition. Bei Linux-ähnlichen Systemen gibt es jedoch nur *eine* systemweite Verzeichnishierarchie, die mehrere Partitionen umfassen kann. Der Schlüssel hierzu ist der Mount-Punkt. Wenn ein Dateisystem gemounted ist, wird das Dateisystem als Satz an Unterverzeichnissen unter dem bestimmten Mount-Punkt zur Verfügung gestellt.

Dieser anscheinende Nachteil ist in Wirklichkeit seine Stärke. Es bedeutet, dass eine nahtlose Erweiterung eines Linux-Dateisystems möglich ist, bei der jedes Verzeichnis als Mount-Punkt für zusätzlichen Festplattenplatz agiert.

Nehmen wir beispielsweise an, dass ein Red Hat Enterprise Linux-System ein Verzeichnis `foo` in seinem Root-Verzeichnis enthält; der vollständige Pfad zu diesem Verzeichnis wäre dann `/foo/`.

Nehmen wir als nächstes an, dass dieses System eine Partition besitzt, die gemountet werden soll, und das der Mount-Punkt dieser Partition `/foo/` sein soll. Besitzt diese Partition eine Datei mit dem Namen `bar.txt` im obersten Verzeichnis, können Sie mit der folgenden vollständigen Dateiangabe auf die Datei zugreifen, nach dem die Partition gemountet wurde:

```
/foo/bar.txt
```

Mit anderen Worten, wenn die Partition gemountet wurde, kann jede Datei, die irgendwo im Verzeichnis `/foo/` gelesen oder geschrieben werden kann, von dieser Partition gelesen oder geschrieben werden.

Ein häufig-verwendeter Mount-Punkt auf vielen Red Hat Enterprise Linux-Systemen ist `/home/` — aus dem Grund, dass sich die Anmeldeverzeichnisse für alle Benutzeraccounts normalerweise unter `/home/` befinden. Wenn `/home/` als Mount-Punkt verwendet wird, werden alle Benutzerdateien auf eine bestimmte Partition geschrieben und füllen nicht das Dateisystem des Betriebssystems.

Tipp

Da ein Mount-Punkt nur ein normales Verzeichnis ist, können Dateien in ein Verzeichnis geschrieben werden, das später als Mount-Punkt verwendet werden soll. Was passiert in diesem Fall mit den Dateien, die sich ursprünglich in diesem Verzeichnis befanden?

Solange die Partition auf diesem Verzeichnis gemountet ist, sind die Dateien nicht zugreifbar (das gemountete Dateisystem erscheint anstelle der Verzeichnisinhalte). Die Dateien werden jedoch nicht beschädigt und könnten nach dem Unmounten der Partition wieder verwendet werden.

5.9.3.2. Anzeigen, was gemountet ist

Zusätzlich zum Mounten und Unmounten von Festplattenplatz können Sie sich anzeigen lassen, was gemountet ist. Es gibt hierfür verschiedene Methoden:

- `/etc/mtab` ansehen
- `/proc/mounts` ansehen
- Den Befehl `df` eingeben

5.9.3.2.1. `/etc/mtab` ansehen

Die Datei `/etc/mtab` ist eine normale Datei, die vom `mount`-Programm aktualisiert wird, wenn Dateisysteme gemountet oder unmountet werden. Hier ein Beispiel für `/etc/mtab`:

```
/dev/sda3 / ext3 rw 0 0
none /proc proc rw 0 0
usbdevfs /proc/bus/usb usbdevfs rw 0 0
/dev/sda1 /boot ext3 rw 0 0
none /dev/pts devpts rw,gid=5,mode=620 0 0
/dev/sda4 /home ext3 rw 0 0
none /dev/shm tmpfs rw 0 0
none /proc/sys/fs/binfmt_misc binfmt_misc rw 0 0
```

Anmerkung

Die Datei `/etc/mtab` ist nur für das Anzeigen des Status zur Zeit gemounteter Dateisysteme gedacht. Sie sollte nicht manuell geändert werden.

Jede Zeile steht für ein Dateisystem, das zur Zeit gemountet ist, und enthält die folgenden Felder (von links nach rechts):

- Gerätespezifikation
- Mount-Punkt
- Dateisystemtyp
- Ob das Dateisystem als nur-lesbar (`ro`) oder lese-/schreibbar (`rw`) gemountet ist, zusammen mit weiteren Mount-Optionen
- Zwei ungenutzte Felder mit Nullen (für Kompatibilität mit `/etc/fstab`[11])

5.9.3.2.2. `/proc/mounts` ansehen

Die Datei `/proc/mounts` ist Teil des Proc-Virtuellen Dateisystems. Wie bei anderen Dateien unter `/proc/` existiert die `mounts` "Datei" auf keiner Festplatte auf Ihrem Red Hat Enterprise Linux-System.

Dies ist eigentlich auch gar keine Datei, sondern eine Repräsentation des Systemstatus, der in Datei-Form (vom Linux-Kernel) zur Verfügung gestellt wird.

Mit dem Befehl `cat /proc/mounts` können wir den Status aller gemounteten Dateisysteme betrachten:

```
rootfs / rootfs rw 0 0
/dev/root / ext3 rw 0 0
/proc /proc proc rw 0 0
usbdevfs /proc/bus/usb usbdevfs rw 0 0
/dev/sda1 /boot ext3 rw 0 0
none /dev/pts devpts rw 0 0
/dev/sda4 /home ext3 rw 0 0
none /dev/shm tmpfs rw 0 0
none /proc/sys/fs/binfmt_misc binfmt_misc rw 0 0
```

Wie Sie im obigen Beispiel sehen können, ist das Format von `/proc/mounts` ähnlich dem des `/etc/mtab`. Es sind eine Reihe von Dateisystemen gemountet, die nichts mit den Festplatten zu tun haben. Unter diesen befinden sich die Dateisysteme `/proc/` (zusammen mit zwei anderen Dateisystemen, die unter `/proc/` gemountet sind), pseudo-ttys und Shared-Memory.

Während das Format zugegebenerweise nicht sehr benutzerfreundlich ist, ist das Anzeigen von `/proc/mounts` der beste Weg, 100% sicherzustellen, das alles, was auf Ihrem Red Hat Enterprise Linux-System gemountet ist angezeigt wird, da diese Informationen vom Kernel bereitgestellt werden. Andere Methoden können unter seltenen Umständen ungenau sein.

Meistens werden Sie jedoch einen Befehl verwenden, der ein leichter lesbares (und daher nützlicheres) Output liefert. Im nächsten Abschnitt wird dieser Befehl beschrieben.

11. Siehe Abschnitt 5.9.5 für weiter Informationen.

5.9.3.2.3. Den Befehl `df` eingeben

Während das Verwenden von `/etc/mtab` oder `/proc/mounts` Ihnen anzeigt, welche Dateisystemen zur Zeit gemountet sind, tut es darüberhinaus wenig. Meistens sind Sie eher an bestimmten Aspekten eines Dateisystems, das gerade gemountet ist, interessiert — dem freien Speicherplatz auf diesem.

Hierfür können wir den Befehl `df` verwenden. Hier eine Beispielausgabe von `df`:

```
Filesystem           1k-blocks      Used Available Use% Mounted on
/dev/sda3              8428196   4280980   3719084  54% /
/dev/sda1               124427     18815     99188  16% /boot
/dev/sda4              8428196   4094232   3905832  52% /home
none                    644600         0    644600   0% /dev/shm
```

Es sind einige Unterschiede zwischen `/etc/mtab` und `/proc/mount` erkennbar:

- Ein leicht lesbarer Header wird angezeigt
- Mit der Ausnahme des Shared-Speichersystems werden nur Festplatten-basierte Dateisysteme angezeigt
- Gesamtgröße, belegter Speicherplatz, freier Speicherplatz und prozentuelle Nutzungszahlen werden angezeigt

Der letzte Punkt ist der wahrscheinlich Wichtigste, da jeder Systemadministrator irgendwann mit einem System zu tun hat, das keinen freien Festplattenplatz mehr hat. Mit `df` können Sie leicht erkennen, wo genau das Problem liegt.

5.9.4. Netzwerk-zugänglicher Speicher unter Red Hat Enterprise Linux

Es gibt zwei Haupttechnologien für das Implementieren von netzwerk-zugänglichem Speicher unter Red Hat Enterprise Linux:

- NFS
- SMB

Die folgenden Abschnitte beschreiben diese Technologien.

5.9.4.1. NFS

Wie der Name besagt, ist das Network File System (NFS; Netzwerk-Dateisystem) ein Dateisystem, auf das über das Netzwerk zugegriffen werden kann. Bei anderen Dateisystemen muss das Speichergerät direkt an das lokale System angeschlossen sein. Bei NFS ist dies jedoch nicht nötig, was eine Vielzahl von Konfigurationen, von zentralisierten Dateisystem-Servern bis zu CD- und Diskettenlosen Computersystemen, ermöglicht.

Im Gegensatz zu anderen Dateisystemen schreibt NFS kein spezifisches Dateiformat vor. Stattdessen verlässt es sich auf den nativen Dateisystemsupport des Server-Betriebssystems, um den eigentlichen I/O auf die lokale Festplatte zu steuern. NFS stellt dann das Dateisystem für alle anderen Betriebssysteme, die einen kompatiblen NFS-Client verwenden, zur Verfügung.

Während dies hauptsächlich eine Linux und UNIX-Technologie ist, ist es erwähnenswert, dass NFS Client Implementierungen auch für andere Betriebssysteme erhältlich sind, was NFS zu einer guten Methode zum Verwenden von Dateien über eine Anzahl verschiedener Plattformen macht.

Das Dateisystem, das ein NFS-Server seinen Clients zur Verfügung stellt, wird durch die Konfigurationsdatei `/etc/exports` gesteuert. Weitere Informationen finden Sie auf den man-Seiten zu `exports(5)` und im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

5.9.4.2. SMB

SMB steht für *Server Message Block* (Server-Nachrichten-Block) und ist der Name für das Kommunikationsprotokoll, das von verschiedenen, von Microsoft hergestellten Betriebssystemen verwendet wird. SMB ermöglicht es, Speicher über das Netzwerk gemeinsam zu verwenden. Moderne Implementierungen verwenden häufig TCP/IP als zugrundeliegenden Transport; vorher war dies NetBEUI.

Red Hat Enterprise Linux unterstützt SMB über das Samba Serverprogramm. Das *Red Hat Enterprise Linux Handbuch zur System-Administration* enthält Informationen zur Konfiguration von Samba.

5.9.5. Dateisysteme automatisch mit `/etc/fstab` mounten

Wenn ein Red Hat Enterprise Linux-System neu installiert wird und dabei alle Festplattenpartitionen erstellt oder definiert wurden, so werden diese dahingehend konfiguriert, dass diese automatisch gemountet werden, wenn das System bootet. Was passiert jedoch, wenn Festplatten hinzugefügt werden, nachdem die Installation abgeschlossen ist? Die Antwort ist "nichts", da das System nicht konfiguriert wurde, diese automatisch zu mounten. Dies kann jedoch leicht geändert werden.

Die Antwort liegt in der `/etc/fstab`-Datei. Diese Datei wird zur Kontrolle, welche Dateisysteme gemountet sind wenn das System bootet, verwendet sowie für das Bereitstellen von Standardwerten für andere Dateisysteme, die eventuell manuell gemountet werden. Hier ein Beispiel für `/etc/fstab`:

```
LABEL=/                 /                       ext3    defaults        1 1
/dev/sda1               /boot                   ext3    defaults        1 2
/dev/cdrom              /mnt/cdrom              iso9660 noauto,owner,kudzu,ro 0 0
/dev/homedisk           /home                   ext3    defaults        1 2
/dev/sda2               swap                    swap    defaults        0 0
```

Jede Zeile repräsentiert ein Dateisystem und enthält die folgenden Felder:

- Dateisystemangabe — Für Festplatten-basierte Dateisysteme entweder ein Gerätedateiname (`/dev/sda1`), eine Dateisystem-Labelspezifikation (`LABEL=/`) oder ein von `devlabel` verwalteter symbolischer Link (`/dev/homedisk`)
- Mount-Punkt — Swap-Partitionen ausgenommen, definiert dieses Feld den Mount-Punkt, der verwendet werden soll, wenn das Dateisystem gemountet wird (`/boot`)
- Dateisystemtyp — Der Typ des Dateisystems, der auf dem angegebenen Gerät existiert (beachten Sie, dass `auto` angegeben werden kann, um automatische Erkennung des zu mountenten Dateisystems auszuwählen, was für tragbare Medien wie Diskettenlaufwerke nützlich ist)
- Mount-Optionen — Eine durch Beistriche getrennte Liste von Optionen, die zum Steuern des `mount`'-Verhaltens verwendet werden kann (`noauto,owner,kudzu`)
- Dump-Häufigkeit — Wird die `dump` Backup-Utility verwendet, steuert die Zahl in diesem Feld das `dump`'-Verhalten auf dem angegebenen Dateisystem
- Dateisystemcheck-Reihenfolge — Regelt die Reihenfolge, in der der Dateisystemprüfer `fsck` die Integrität des Dateisystems prüft

5.9.6. Speicher hinzufügen/löschen

Während die meisten dieser Schritte, die für das Hinzufügen oder Entfernen von Speicher nötig sind, eher von der Systemhardware als der Systemsoftware abhängen, gibt es dennoch Aspekte dieser Vorgänge, die für die jeweilige Betriebsumgebung spezifisch sind. In diesem Abschnitt werden die Schritte für das Hinzufügen und Entfernen von Speicher behandelt, die auf Red Hat Enterprise Linux zugeschnitten sind.

5.9.6.1. Speicher hinzufügen

Das Hinzufügen von Speicher zu einem Red Hat Enterprise Linux-System ist relativ einfach. Hier die Schritte, die für Red Hat Enterprise Linux spezifisch sind:

- Partitionieren
- Partitionen formatieren
- `/etc/fstab` aktualisieren

Die folgenden Abschnitte erklären jeden Schritt im Detail.

5.9.6.1.1. Partitionieren

Sobald die Festplatte installiert wurde, ist es nötig, eine oder mehr Partitionen zu erstellen, um den Speicherplatz für Red Hat Enterprise Linux zur Verfügung zu stellen.

Es gibt hierfür mehr als einen Weg:

- Mit dem Befehlszeilen-basierten `fdisk` Utility-Programm
- Mittels `parted`, ein weiteres Befehlszeilen-basiertes Utility-Programm

Auch wenn sich die Tools unterscheiden, sind die grundlegenden Schritte die gleichen. Das folgende Beispiel enthält die Befehle, die für das Ausführen der Schritte mit `fdisk` nötig sind:

1. Wählen Sie die neue Festplatte (der name der Festplatte kann durch die Namenskonventionen wie in Abschnitt 5.9.1 beschrieben herausgefunden werden). Mit `fdisk` geschieht dies, indem Sie den Gerätenamen angeben, wenn Sie `fdisk` starten:
   `fdisk /dev/hda`

2. Sehen Sie sich die Partitionstabelle der Festplatte an, um sicherzustellen, dass das zu partitionierende Gerät auch wirklich das Richtige ist. In unserem Beispiel zeigt `fdisk` die Partitionstabelle mittelsdem Befehl `p` an:
   ```
   Command (m for help): p

   Disk /dev/hda: 255 heads, 63 sectors, 1244 cylinders
   Units = cylinders of 16065 * 512 bytes

      Device Boot    Start       End    Blocks   Id  System
   /dev/hda1   *         1        17    136521   83  Linux
   /dev/hda2            18        83    530145   82  Linux swap
   /dev/hda3            84       475   3148740   83  Linux
   /dev/hda4           476      1244   6176992+  83  Linux
   ```

3. Löschen Sie alle unerwünschten Partitionen, die eventuell bereits auf der neuen Festplatte vorhanden sind. Verwenden Sie hierfür den Befehl `d` in`fdisk`:
   ```
   Command (m for help): d
   Partition number (1-4): 1
   ```
   Dieser Vorgang muss für alle nicht benötigten Partitionen auf der Festplatte wiederholt werden.

4. Erstellen Sie die neue Partition, geben Sie die gewünschte Größe und den Dateisystemtyp an. Mit `fdisk` umfasst dies zwei Schritte — Erstens das Erstellen der Partition (mit dem Befehl `n`):
   ```
   Command (m for help): n
   Command action
      e   extended
      p   primary partition (1-4)

   p
   ```

```
Partition number (1-4): 1
First cylinder (1-767): 1
Last cylinder or +size or +sizeM or +sizeK: +512M
```

Zweitens das Einstellen des Dateisystemtyps (mit dem Befehl `t`):

```
Command (m for help): t
Partition number (1-4): 1
Hex code (type L to list codes): 82
```

Partitionstyp 82 stellt eine Linux Swap-Partition dar.

5. Speichern Sie Ihre Änderungen und verlassen Sie das Partitionierungs-Programm. Unter `fdisk` geschieht dies mit dem Befehl `w`:

```
Command (m for help): w
```

Achtung

Bei der Partitionierung einer neuen Festplatte ist es *wichtig*, dass Sie sicher sind, das Sie die richtige Festplatte partitionieren. Ansonsten laufen Sie Gefahr, eine Festplatte zu partitionieren, die bereits verwendet wird, was in Datenverlust endet.

Stellen Sie auch sicher, dass Sie die beste Partitionsgröße gewählt haben. Überlegen Sie sich dies gut, denn ein nachträgliches Ändern ist wesentlich schwieriger als sich jetzt ein bisschen Zeit zu nehmen um dies zu durchdenken.

5.9.6.1.2. Partitionen formatieren

Das Formatieren von Partitionen unter Red Hat Enterprise Linux geschieht mit dem `mkfs` Utility-Programm. `mkfs` schreibt jedoch nicht die eigentlichen Dateisystem-spezifischen Informationen auf die Festplatte, sondern gibt die Kontrolle an eines von mehreren anderen Programmen weiter, die dann das Dateisystem erstellen.

Lesen Sie nun die `mkfs.`<*`fstype`*> man-Seite für das von Ihnen gewählte Dateisystem. Betrachten Sie zum Beispiel die `mkfs.ext3` man-Seite für die Optionen beim Erstellen eines neuen ext3-Dateisystems. Im Allgemeinen bietet das `mkfs.`<*`fstype`*>-Programm gute Standardwerte für die meisten Konfigurationen. Es gibt jedoch Optionen, die häufig von Systemadministratoren geändert werden:

- Das Einstellen eines Volumen-Labels für spätere Verwendung in `/etc/fstab`
- Das Einstellen eines geringeren Prozentsatzes an reserviertem Speicherplatz für den Super-User auf sehr großen Festplatten
- Das Einstellen einer nicht-standardmäßigen Blockgröße und/oder Bytes pro Inode für Konfigurationen, die entweder sehr große oder sehr kleine Dateien unterstützen müssen
- Das Prüfen auf defekte Blöcke vor dem Formatieren

Wenn die Dateisysteme für alle jeweiligen Partitionen erstellt wurden, ist die Festplatte richtig für den Einsatz konfiguriert.

Als nächstes sollten Sie grundsätzlich nocheinmal Ihre Arbeit prüfen, indem Sie die Partitionen manuell mounten und sicherstellen, dass alles funktioniert. Ist alles in Ordnung, können Sie nun Ihr Red Hat Enterprise Linux-System so konfigurieren, dass die neuen Dateisysteme automatisch gemountet werden , wenn das System bootet.

5.9.6.1.3. `/etc/fstab` aktualisieren

Wie unter Abschnitt 5.9.5 beschrieben, müssen Sie die nötigen Zeilen zu `/etc/fstab` hinzufügen, im sicherzustellen, dass die neuen Dateisysteme beim Booten des Systems gemountet werden. Sobald Sie `/etc/fstab` aktualisiert haben, testen Sie dies, in dem Sie einen "unvollständigen" `mount` ausführen, bei dem Sie nur das Gerät oder Mount-Punkt angeben. Einer der folgenden Befehle reicht aus:

```
mount /home
mount /dev/hda3
```

(Ersetzen Sie `/home` oder `/dev/hda3` mit dem Mount-Punkt oder Gerät für Ihre Situation.)

Ist der jeweilige `/etc/fstab`-Eintrag richtig, findet `mount` die fehlenden Informationen und schließt den Mount-Vorgang ab.

Sie können jetzt ziemlich sicher sein, dass `/etc/fstab` richtig konfiguriert ist, um den neuen Speicher beim Booten des Systems zu mounten (wenn Sie Zeit für einen schnellen Neustart haben, ist dies sicher nicht verkehrt — nur um sicher zu gehen).

5.9.6.2. Speicher entfernen

Das Entfernen von Speicher von einem Red Hat Enterprise Linux-System ist relativ einfach. Hier die Schritte spezifisch für Red Hat Enterprise Linux:

- Entfernen Sie die Festplatten-Partitionen von `/etc/fstab`
- Unmounten Sie die aktiven Partitionen der Festplatte
- Löschen Sie den Inhalt der Festplatte

Die folgenden Abschnitte beschreiben diesen Vorgang näher.

5.9.6.2.1. Entfernen Sie die Partitionen von `/etc/fstab`

Entfernen Sie in einem Texteditor Ihrer Wahl die Zeilen für die Festplattenpartitionen in der Datei `/etc/fstab`. Sie finden die richtigen Zeilen mit einer der folgenden Methoden:

- Vergleichen Sie den Mount-Punkt der Partition mit dem Verzeichnis in der zweiten Spalte von `/etc/fstab`
- Vergleichen Sie den Gerätedateinamen mit den Dateinamen in der ersten Spalte von `/etc/fstab`

Tipp

Suchen Sie alle Zeilen in `/etc/fstab`, die Swap-Partitionen auf der zu entfernenden Festplatte angeben; diese können leicht übersehen werden.

5.9.6.2.2. Zugriff mit `umount` beenden

Beenden Sie jeglichen Zugriff zu der Festplatte. Für Partitionen mit aktiven Dateisystemen verwenden Sie den Befehl `umount`. Gibt es auf der Festplatte eine Swap-Partition, muss diese entweder mit dem Befehl `swapoff` deaktiviert oder das System neu gebootet werden.

Das Unmounten der Partitionen mit dem Befehl `umount` erfordert, dass Sie entweder den Gerätedateinamen oder den Mount-Punkt der Partition angeben:

```
umount /dev/hda2
umount /home
```

Eine Partition kann nur ungemountet werden, wenn diese zur Zeit nicht verwendet wird. Kann die Partition im normalen Runlevel nicht ungemountet werden, booten Sie in den Rettungsmodus und entfernen Sie den Eintrag für die Partition in der `/etc/fstab`-Datei.

Wenn Sie `swapoff` für das Deaktivieren des Swapping zu einer Partition verwenden, müssen Sie den Gerätedateinamen, der die Swap-Partition darstellt, angeben:

```
swapoff /dev/hda4
```

Kann das Swapping zu einer Partition über `swapoff` nicht deaktiviert werden, booten Sie in den Rettungsmodus und entfernen Sie den Eintrag in `/etc/fstab`.

5.9.6.2.3. Inhalte der Festplatte löschen

Das Löschen des Festplatteninhalts unter Red Hat Enterprise Linux ist einfach.

Nachdem Sie alle Partitionen der Festplatte ungemountet haben, geben Sie als root den folgenden Befehl ein:

```
badblocks -ws <device-name>
```

<*device-name*> steht für den Dateinamen der Festplatte, die Sie löschen möchten, exklusive der Partitionsnummer. Zum Beispiel `/dev/hdb` für die zweite ATA-Festplatte.

Die folgende Ausgabe wird angezeigt, während `badblocks` läuft:

```
Writing pattern 0xaaaaaaaa: done
Reading and comparing: done
Writing pattern 0x55555555: done
Reading and comparing: done
Writing pattern 0xffffffff: done
Reading and comparing: done
Writing pattern 0x00000000: done
Reading and comparing: done
```

Denken Sie daran, dass `badblocks` vier verschiedene Datenmuster auf jeden Block auf der Festplatte schreibt. Bei großen Festplatten kann dies dauern — häufig mehrere Stunden.

Wichtig

Viele Unternehmen (und Behörden) haben spezielle Methoden für das Löschen von Daten auf Festplatten und anderen Speichermedien. Sie sollten *immer* sicherstellen, dass Sie diese Anforderungen verstehen und diese befolgen. In vielen Fällen gibt es rechtliche Auswirkungen, wenn Sie dies nicht tun. Das obige Beispiel sollten keinesfalls als die einzige Methode zum Löschen einer Festplatte betrachtet werden.

Es ist jedoch wesentlich effektiver als der `rm`-Befehl. Beim Löschen einer Datei mit dem `rm`-Befehl wird die Datei als gelöscht markiert — der Inhalt der Datei wird jedoch *nicht* gelöscht.

5.9.7. Festplattenquoten implementieren

Red Hat Enterprise Linux kann durch den Einsatz von Festplattenquoten die Verwendung von Festplattenplatz auf Benutzer- und Gruppen-Basis prüfen. Der folgende Abschnitt bietet einen Überblick über die Festplattenquoten-Funktionen unter Red Hat Enterprise Linux.

5.9.7.1. Hintergrund zu Festplattenquoten

Festplattenquoten unter Red Hat Enterprise Linux haben die folgenden Eigenschaften:

- Pro-Dateisystem Implementierung
- Haushaltung des verfügbaren Speicherplatzes pro Benutzer
- Haushaltung des verfügbaren Speicherplatzes pro Gruppe
- Blocknutzung der Festplatte aufzeichnen
- Inode-Nutzung der Festplatte aufzeichnen
- Feste Grenzen
- Weiche Grenzen
- Gnadenfristen

Die folgenden Abschnitte beschrieben jede dieser Eigenschaften näher.

5.9.7.1.1. Pro-Dateisystem Implementierung

Festplattenquoten unter Red Hat Enterprise Linux können auf einer Pro-Dateisystem-Basis eingesetzt werden. In anderen Worten können Festplattenquoten individuell für jedes einzelen Dateisystem aktiviert oder deaktiviert werden.

Dies bietet dem Systemadministrator sehr viel Flexibilität. Wenn sich zum Beispiel das `/home/`-Verzeichnis auf einem eigenen Dateisystem befindet, können hier Festplattenquoten aktiviert werden, was eine gleichmäßige Verwendung des Platzes von allen Benutzern ermöglicht. Das root-Dateisystem könnte jedoch ohne Festplattenquoten belassen werden, was die Komplexität der Wartung von Quoten auf einem Dateisystem, auf dem sich nur das Betriebssystem befindet, eliminiert.

5.9.7.1.2. Haushaltung des verfügbaren Speicherplatzes pro Benutzer

Festplattenquoten können die Haushaltung verfügbaren Speicherplatzes auf einer Pro-Benutzer-Basis regeln. Dies bedeutet, dass die Verwendung des Platzes pro Benutzer individuell verwaltet wird. Dies bedeutet auch, dass jegliche Einschränkungen (die in späteren Abschnitten beschrieben werden) auch auf Benutzer-Basis verwaltet werden.

Die Flexibilität des Verfolgens und Erzwingens von Festplattenverwendung pro Benutzer ermöglicht es Systemadministratoren, verschiedene Grenzen für individuelle Benutzer, gemäß deren Verantwortung und Speicherbedarf, zu vergeben.

5.9.7.1.3. Haushaltung des verfügbaren Speicherplatzes pro Gruppe

Festplattenquoten können die Festplattenverwendung auch auf Gruppen-Basis verfolgen. Dies ist ideal für Unternehmen, die Gruppen als Kombination verschiedener Benutzer für eine einzige, projektweite Ressource einsetzen.

Indem Gruppen-weite Festplattenquoten festgelegt werden, können Administratoren die Speicherverwendung genau verwalten, indem einzelnen Benutzern nur die Quote für deren persönliche Verwendung zugewiesen wird, während größere Quoten, die für Multi-Benutzer-Projekte

geeigneter sind, gesetzt werden können. Dies ist ein großer Vorteil für Unternehmen, die einen "Chargeback"-Mechanismus verwenden, bei dem die Datenzentrum-Kosten den Abteilungen und Teams auf Basis der Verwendung von Ressourcen zugeteilt werden.

5.9.7.1.4. Blocknutzung der Festplatte aufzeichnen

Festplattenquoten dienen zum Nachverfolgen der Verwendung von Festplattenblöcken. Da alle Daten auf einem Dateisystem in Blöcken gespeichert werden, können Festplattenquoten die erstellten und gelöschten Dateien auf einem Dateisystem in direktem Bezug setzen mit der Größe des Speichers, den die Dateien in Anspruch nehmen.

5.9.7.1.5. Inode-Nutzung der Festplatte aufzeichnen

Zusätzlich dazu können Festplattenquoten auch die Inode-Verwendung verfolgen. Unter Red Hat Enterprise Linux speichern Inodes verschiedene Teile des Dateisystems. Am wichtigsten ist jedoch die Tatsache, dass Inodes die Informationen für jede Datei halten. Durch das Verfolgen (und Steuern) der Inode-Verwendung ist es möglich, die Erstellung neuer Dateien zu kontrollieren.

5.9.7.1.6. "Harte" Grenzen

Eine harte Grenze ist die maximale Anzahl an Festplattenblöcken (oder Inodes), die temporär von einem Benutzer (oder einer Gruppe) verwendet werden kann. Jeglicher Versuch, auch nur einen Block über der harten Grenze zu verwenden, schlägt fehl.

5.9.7.1.7. "Weiche" Grenzen

Eine weiche Grenze ist die maximale Anzahl von Festplattenblöcken, die von einem Benutzer (oder Gruppe) permanent verwendet werden kann.

Die weiche Grenze liegt unter der harten Grenze, Dies ermöglicht Benutzern, deren weiche Grenze temporär zu überschreiten, was diesen ermöglicht, deren Arbeit fertigzustellen und deren Dateien durchzusehen und die Verwendung wieder unterhalb der weichen Grenze zu bringen.

5.9.7.1.8. Gnadenfristen

Wie schon erwähnt ist die Festplattenverwendung überhalb der weichen Grenze temporär. Es ist die Gnadenfrist, die festlegt, wie lange ein Benutzer (oder eine Gruppe) die Verwendung von Speicher überhalb der weichen Grenze bis hin zur harten Grenze fortsetzen kann.

Verwendet ein Benutzer dauerhaft mehr Speicher, als durch die weiche Grenze festgelegt und die Gnadenfrist läuft ab, wird solange kein weiterer Speicher zur Verfügung gestellt, bis der Benutzer (oder Gruppe) dessen/deren Verwendung auf ein Maß unterhalb der weichen Grenze reduziert hat.

Die Gnadenfrist kann in Sekunden, Minuten, Stunden, Tagen, Wochen oder Monaten ausgesprochen werden, was dem Systemadministrator eine gewisse Freiheit in der Festlegung der der Zeiträume gibt.

5.9.7.2. Festplattenquoten aktivieren

Anmerkung

Im folgenden Abschnitt werden die nötigen Schritte für das Aktivieren von Festplattenquoten unter Red Hat Enterprise Linux kurz beschrieben. Eine tiefergehende Beschreibung dieses Themas finden Sie im Kapitel über Festplattenquoten im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Um Festplattenquoten nutzen zu können, müssen Sie diese aktivieren. Dies umfasst mehrere Schritte:

1. `/etc/fstab` ändern
2. Dateisysteme erneut mounten
3. `quotacheck` ausführen
4. Quoten zuweisen

Die Datei `/etc/fstab` kontrolliert das Mounten von Dateisystemen unter Red Hat Enterprise Linux. Da Festplattenquoten auf einer Pro-Dateisystem-Basis vergeben werden, gibt es zwei Optionen — `usrquota` und `grpquota` — die zu der Datei hinzugefügt werden müssen, um Festplatten zu aktivieren.

Die Option `usrquota` aktiviert Benutzer-basierte Festplattenquoten, während `grpquota` Gruppen-basierte Quoten aktiviert. Es können eine oder beide dieser Optionen aktiviert werden, indem diese in das Optionsfeld für das gewünschte Dateisystem eingetragen werden.

Die betroffenen Dateisysteme müssen dann ungemountet und neu gemountet werden, damit die Festplatten-bezogenen Optionen wirksam werden.

Als nächstes wird der Befehl `quotacheck` verwendet, um die Festplattenquotendateien zu erstellen und die aktuellen Verwendungsdaten von bereits bestehenden Dateien zu sammeln. Die Festplattenquotendateien (`aquota.user` und `aquota.group` für Benutzer- und Gruppen-basierte Quoten) enthalten die nötigen Quoten-bezogenen Informationen und befinden sich im root-Verzeichnis des Systems.

Um Festplattenquoten zuzuweisen, verwenden Sie den Befehl `edquota`.

Dieses Utility-Programm verwendet einen Texteditor für das Anzeigen der Quoteninformationen für den Benutzer oder die Gruppe als Teil des `edquota` Befehls. Hier ein Beispiel:

```
Disk quotas for user matt (uid 500):
  Filesystem      blocks       soft       hard     inodes     soft     hard
  /dev/md3       6618000          0          0      17397        0        0
```

Dies zeigt, dass der Benutzer "matt" über 6 GB Festplattenplatz und mehr als 17 000 Inodes verwendet. Es wurde bisher keine Quote (weich oder hart) für Festplattenblöcke oder Inodes gesetzt, was bedeutet, dass es keine Grenze für den Festplattenplatz und Inodes, die dieser Benutzer verwenden kann, gibt.

Mit dem Texteditor, der die Festplattenquoten-Informationen anzeigt, kann der Systemadministrator nun die weichen und harten Grenzen nach Belieben einstellen:

```
Disk quotas for user matt (uid 500):
  Filesystem      blocks       soft       hard     inodes     soft     hard
  /dev/md3       6618000    6900000    7000000      17397        0        0
```

In diesem Beispiel wurde dem Benutzer "matt" eine weiche Grenze von 6,9 GB und eine harte Grenze von 7 GB zugewiesen. Es wurden keine weichen oder harten Grenzen für die Inodes gesetzt.

Tipp

Das `edquota`-Programm kann auch zum Einstellen der pro-Datei Gnadenfrist mittels der Option `-t` genutzt werden.

5.9.7.3. Festplattenquoten verwalten

Es bedarf nur wenig Verwaltung für die Unterstützung von Festplattenquoten unter Red Hat Enterprise Linux. Im Grunde ist alles, was benötigt wird:

- Das Generieren von Verwendungsberichten in regelmäßigen Abständen (und die Absprache mit Benutzern, die anscheinend Probleme haben, den ihnen zugewiesenen Festplattenplatz zu verwalten)
- Das Sicherstellen, dass die Festplattenquoten genau bleiben

Das Erstellen eines Verwendungsberichts erfordert das Ausführen des Utility-Programms `repquota`. Der Befehl `repquota /home` produziert folgende Ausgabe:

```
*** Report for user quotas on device /dev/md3
Block grace time: 7days; Inode grace time: 7days
                        Block limits                File limits
User            used    soft    hard  grace    used  soft  hard  grace
----------------------------------------------------------------------
root      --   32836       0       0              4     0     0
matt      -- 6618000 6900000 7000000          17397     0     0
```

Weitere Informationen zu `repquota` finden Sie im *Red Hat Enterprise Linux Handbuch zur System-Administration* im Kapitel zu den Festplattenquoten.

Wenn ein Dateisystem nicht ordnungsgemäß ungemountet wird (z.B. durch einen Systemabsturz), ist es notwendig, `quotacheck` auszuführen. Viele Systemadministratoren empfehlen jedoch das Ausführen von `quotacheck` auf regelmäßiger Basis, auch wenn das System nicht abgestürzt ist.

Dieser Vorgang ist ähnlich der anfänglichen Verwendung von `quotacheck`, wenn Festplattenquoten aktiviert werden.

Hier ein Beispielbefehl für `quotacheck`:

```
quotacheck -avug
```

Am einfachsten wird `quotacheck` auf regelmäßiger Basis mit`cron` ausgeführt. Die meisten Systemadministratoren führen `quotacheck` einmal pro Woche aus. Sie können jedoch auch ganz nach Bedarf und entsprechend den Umständen längere oder kürzere Intervalle auswählen.

5.9.8. RAID-Arrays erstellen

Zusätzlich zur Unterstützung von Hardware-RAID-Lösungen unterstützt Red Hat Enterprise Linux Software RAID. Ein Software-RAID kann auf zwei Arten erstellt werden:

- Während der Installation von Red Hat Enterprise Linux

- Nach der Installation von Red Hat Enterprise Linux

Die folgenden Abschnitte stellen diese beiden Methoden vor.

5.9.8.1. Während der Installation von Red Hat Enterprise Linux

Während des normalen Red Hat Enterprise Linux Installationsvorgangs kann ein RAID-Array erstellt werden. Dies wird während des Festplatten-Partitionierungsphase der Installation ausgeführt.

Sie müssen zuerst Ihre Festplatten manuell mit **Disk Druid** partitionieren. Sie müssen eine neue Partition des Typs "Software RAID" erstellen. Dann wählen Sie die Festplatten, die Teil des RAID-Arrays sein sollen, aus dem Feld **zulässige Festplatten** aus. Wählen Sie dann die gewünschte Größe und ob diese Partition eine Primärpartition sein soll.

Wenn Sie alle Partitionen, die für das RAID-Array benötigt werden, erstellt haben, müssen Sie über den Button **RAID** die eigentlichen Arrays erstellen. Sie erhalten dann ein Dialogfeld, in dem Sie die Mount-Punkte, Dateisystemtypen, RAID-Gerätenamen, und die "Software RAID" Partitionen, auf denen das RAID-Array basiert, festlegen können.

Sobald die gewünschten Arrays erstellt wurden, wird der Installationsprozess wie gewohnt fortgeführt.

Tipp

Weitere Informationen zur Erstellung von Software RAID-Arrays während der Installation von Red Hat Enterprise Linux finden Sie im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

5.9.8.2. Nach der Installation von Red Hat Enterprise Linux

Das Erstellen eines RAID-Array nachdem Red Hat Enterprise Linux installiert wurde, ist etwas komplexer. Wie beim Hinzufügen von Speicher muss die nötige Hardware erst installiert und richtig konfiguriert werden.

Das Partitionieren ist auch anders für RAID als für einzelne Festplatten. Anstelle einer Partition des Typs "Linux" (Typ 83) oder "Linux swap" (Typ 82) müssen alle Partitionen, die Teil eines RAID-Arrays sind, auf "Linux raid auto" (Typ fd) gesetzt werden.

Als nächstes muss die Datei `/etc/raidtab` erstellt werden. Diese Datei ist verantwortlich für die richtige Konfiguration aller RAID Arrays auf Ihrem System. Das Dateiformat (das auf der `raidtab(5)` man-Seite dokumentiert ist) ist relativ einfach. Hier ein Beispieleintrag in `/etc/raidtab` für ein RAID 1-Array:

```
raiddev             /dev/md0
raid-level                  1
nr-raid-disks               2
chunk-size                  64k
persistent-superblock       1
nr-spare-disks              0
    device          /dev/hda2
    raid-disk     0
    device          /dev/hdc2
    raid-disk     1
```

Einige der erwähnenswerteren Abschnitte in diesem Eintrag sind:

- `raiddev` — Zeigt den Gerätedateinamen für das RAID-Array[12]
- `raid-level` — Definiert den RAID-Level, der von diesem RAID-Array verwendet werden soll
- `nr-raid-disks` — Zeigt an, wieviele physikalische Festplattenpartitionen Teil dieses Arrays sein sollen
- `nr-spare-disks` — Software-RAID unter Red Hat Enterprise Linux ermöglicht die Definition einer oder mehrerer Ersatz-Partitionen; diese Partitionen können automatisch den Platz einer fehlerhaften Festplatte einnehmen
- `device`, `raid-disk` — Zusammen definieren diese die physikalischen Festplattenpartitionen, aus denen das RAID-Array besteht

Als nächstes müssen Sie das eigentliche RAID-Array erstellen. Dies geschieht mit dem Programm `mkraid`. In unserem Beispiel `/etc/raidtab` würden wir das `/dev/md0` RAID-Array mit dem folgenden Befehl erstellen:

```
mkraid /dev/md0
```

Das RAID-Array `/dev/md0` kann jetzt formatiert und gemountet werden. Der Vorgang unterscheidet sich nicht vom Formatieren und Mounten einer einzelnen Festplatte.

5.9.9. Tägliche Verwaltung des RAID-Arrays

Es gibt wenig, was zum Betrieb eines RAID-Arrays notwendig ist. Solange keine Hardware-Probleme auftreten, sollte das Array wie eine einzelne physikalische Festplatte funktionieren. Wie ein Systemadministrator jedoch den Status aller Festplatten im System prüfen sollte, muss auch der Status des RAID-Arrays geprüft werden.

5.9.9.1. Array-Status prüfen mit `/proc/mdstat`

Die Datei `/proc/mdstat` bietet die einfachste Methode, den Status aller RAID-Arrays auf einem bestimmten System zu prüfen. Hier ein Beispiel-`mdstat` (Anzeige über den Befehl `cat /proc/mdstat`):

```
Personalities : [raid1]
read_ahead 1024 sectors
md1 : active raid1 hda3[0] hdc3[1]
      522048 blocks [2/2] [UU]

md0 : active raid1 hda2[0] hdc2[1]
      4192896 blocks [2/2] [UU]

md2 : active raid1 hda1[0] hdc1[1]
      128384 blocks [2/2] [UU]

unused devices: <none>
```

Auf diesem System befinden sich drei RAID-Arrays (alle RAID 1). Jedes RAID-Array hat seinen eigenen Abschnitt in `/proc/mdstat` und enthält folgende Informationen:

- Den RAID-Array-Gerätenamen (nicht im `/dev/`-Teil enthalten)
- Der Status des RAID-Arrays

12. Bitte beachten Sie, dass der Gerätedateiname des RAID-Arrays nicht Informationen des Partitions-Levels wiederspiegelt, da das RAID-Array aus partitioniertem Festplattenplatz besteht.

- Der RAID-Level des RAID-Arrays
- Die physikalischen Partitionen, aus denen das Array besteht (gefolgt von der Unit-Nummer des Arrays der Partition)
- Die Größe des Arrays
- Die Anzahl der konfigurierten Geräte gegen die Anzahl der funktionstüchtigen Geräte im Array
- Den Status jedes konfigurierten Gerätes im Array (`U` bedeutet das Gerät ist OK und _ zeigt einen Fehler an)

5.9.9.2. RAID Array mit `raidhotadd` neu erstellen

Sollte `/proc/mdstat` anzeigen, dass ein Problem mit einem der RAID-Arrays besteht, sollte das Utility Programm `raidhotadd` zum Neubau des Arrays verwendet werden. Hier die Schritte, die dann ausgeführt werden müssen:

1. Stellen Sie fest, welche Festplatte die ausgefallene Partition enthält
2. Beheben Sie das Problem, das den Ausfall verursacht hat (wahrscheinlich durch Austausch des Geräts)
3. Partitionieren Sie die neue Festplatte, sodass die Partitionen hierauf *identisch* mit denen auf der anderen Festplatte im Array sind
4. Geben Sie den folgenden Befehl ein:
   `raidhotadd <raid-device> <disk-partition>`
5. Überwachen Sie `/proc/mdstat`, ob das Rebuild stattfindet

Tipp

Hier ein Befehl, mit dem Sie den Neuaufbau ansehen können:

```
watch -n1 cat /proc/mdstat
```

Dieser Befehl zeigt den Inhalt von `/proc/mdstat` an und aktualisiert diesen jede Sekunde.

5.9.10. Logical Volume Management (LVM)

Red Hat Enterprise Linux enthält Support für LVM. LVM kann konfiguriert werden, während Red Hat Enterprise Linux installiert wird oder nachdem die Installation abgeschlossen ist. LVM unter Red Hat Enterprise Linux unterstützt die Gruppierung von physikalischem Speicher, Größenänderung der logischen Volumen und die Migration von Daten von einem bestimmten physikalischen Volumen.

Weitere Informationen zu LVM finden Sie unter *Red Hat Enterprise Linux Handbuch zur System-Administration*.

5.10. Zusätzliche Ressourcen

Dieser Abschnitt enthält verschiedene Ressourcen, die zum Thema Speichertechnologien und Red Hat Enterprise Linux-spezifische Informationen konsultiert werden können.

5.10.1. Installierte Dokumentation

Die folgenden Ressourcen werden während einer typischen Red Hat Enterprise Linux-Installation installiert und können Ihnen helfen, mehr über die Themen in diesem Kapitel zu erfahren.

- `exports(5)` man-Seite — Lernen Sie mehr über das NFS-Konfigurationsdatei-Format.
- `fstab(5)` man-Seite — Lernen Sie mehr über Konfigurationsdateiformat für Dateisysteminformationen.
- `swapoff(8)` man-Seite — Lernen Sie Swap-Partitionen zu deaktivieren.
- `df(1)` man-Seite — Lernen Sie die Nutzung des Festplattenplatzes auf gemounteten Dateisystemen darzustellen.
- `fdisk(8)` man-Seite — Lernen Sie mehr über das Utility-Programm zur Wartung der Partitionstabellen.
- `mkfs(8)`, `mke2fs(8)` man-Seiten — Lernen Sie mehr über diese Utility-Programme zur Erstellung von Dateisystemen.
- `badblocks(8)` man-Seite — Lernen Sie ein Gerät auf defekte Blöcke zu testen.
- `quotacheck(8)` man-Seite — Lernen Sie Block- und Inode-Verwendung für Benutzer und Gruppen zu verifizieren und optional Festplattenquoten zu erstellen.
- `edquota(8)` man-Seite — Lernen Sie mehr über das Utility-Programm für die Wartung von Festplattenquoten.
- `repquota(8)` man-Seite — Lernen Sie mehr über das Utility-Programm zum Berichten von Festplattenquoten.
- `raidtab(5)` man-Seite — Lernen Sie mehr über das Format für die Dateikonfiguration des Software RAID.
- `mkraid(8)` man-Seite — Lernen Sie mehr über dieses Utility-Programm für die Software RAID-Array-Erstellung.
- `mdadm(8)` man-Seite — Lernen Sie merh über dieses Utility-Programm für die Software RAID-Array-Verwaltung.
- `lvm(8)` man-Seite — Lernen Sie merh über Logical Volume Management.
- `devlabel(8)` man-Seite — Lernen Sie mehr über den durchgehenden Speichergerät-Zugriff.

5.10.2. Nützliche Webseiten

- http://www.pcguide.com/ — Eine nützliche Site für Informationen zu verschiedenen Speicher-Technologien.
- http://www.tldp.org/ — DasLinux Documentation Project bietet HOWTOs und mini-HOWTOs, die Ihnen einen guten Überblick über Speichertechnologien und deren Bezug zu Linux geben.

5.10.3. Bücher zum Thema

Die folgenden Bücher behandeln verschiedene Themen in Bezug zu Speicher und bieten eine gute Ressource für Red Hat Enterprise Linux Systemadministratoren.

- Das *Red Hat Enterprise Linux Installationshandbuch*; Red Hat, Inc. — Enthält Anweisungen zur Partitionierung von Festplatten während der Installation von Red Hat Enterprise Linux und einen Überblick über Festplattenpartitionen.

- Das *Red Hat Enterprise Linux Referenzhandbuch*; Red Hat, Inc. — Enthält detaillierte Informationen zur Verzeichnisstruktur in Red Hat Enterprise Linux und einen Überblick über NFS.
- Das *Red Hat Enterprise Linux Handbuch zur System-Administration*; Red Hat, Inc. — Enthält Kapitel zu Dateisystemen, RAID, LVM, `devlabel`, Partitionierung, Festplattenquoten, NFS und Samba.
- *Linux System Administration: A User's Guide* von Marcel Gagne; Addison Wesley Professional — Enthält Informationen zu Benutzer- und Gruppenberechtigungen, Dateisystemen und Festplattenquoten, NFS und Samba.
- *Linux Performance Tuning and Capacity Planning* von Jason R. Fink and Matthew D. Sherer; Sams — Enthält Informationen zur Performance von Festplatten, RAID und NFS.
- *Linux Administration Handbook* von Evi Nemeth, Garth Snyder and Trent R. Hein; Prentice Hall — Enthält Informationen zu Dateisystemen, Festplatten, NFS und Samba.

Kapitel 6.

Verwalten von Benutzer-Accounts und Ressourcen-Zugang

Die Verwaltung von *Benutzer-Accounts* und *Gruppen* ist ein wesentlicher Bestandteil der System-Administration innerhalb eines Unternehmens. Um dies jedoch so effizient als möglich zu bewerkstelligen, muss ein guter System-Administrator zuallererst über Benutzer-Accounts und Gruppen genauestens Bescheid wissen.

Der Hauptgrund für die Existenz von Benutzer-Accounts liegt in der eindeutigen Verifizierung der Identität jedes einzelnen Individuums, welches ein Computersystem benutzt. Ein sekundärer (jedoch auch wichtiger) Grund für die Erstellung von Benutzer-Accounts ist die für jeden Einzelnen maßgeschneiderte Vergabe von Resource- und Zugriffspriviligien.

Ressourcen können Dateien, Verzeichnisse und Geräte beinhalten. Den Zugang zu diesen Ressourcen zu kontrollieren, ist ein wesentlicher Bestandteil der täglichen Routine eines Systemadministrators. Oft wird auch der Zugang zu einer Ressource durch Gruppen kontrolliert. Gruppen sind logische Konstrukte, welche dazu benutzt werden Benutzer-Accounts für einen gemeinsamen Zweck zusammenzufassen. Wenn zum Beispiel ein Unternehmen mehrere Systemadministratoren besitzt, so können diese alle einer Systemadministratorengruppe zugeordnet werden. Der Gruppe kann sodann die Erlaubnis erteilt werden auf Schlüsselressourcen des Systems zuzugreifen. Dies macht Gruppen zu einem leistungsfähigen Werkzeug bei der Verwaltung von Ressourcen und Zugriffsberechtigungen.

In den folgenden Abschnitten werden Benutzer-Accounts und Gruppen genauer definiert.

6.1. Verwalten von Benutzer-Accounts

Wie bereits erwähnt, werden Benutzer-Accounts zur Identifikation und Authentifizierung von einzelnen Individuen benutzt. Benutzer-Accounts haben etliche verschiedene Komponenten. Zuallererst gibt es den Benutzernamen. Das Passwort kommt als Nächstes, gefolgt von der Information über die Zugriffskontrolle.

Die folgenden Abschnitte behandeln jede einzelne Komponente im Detail.

6.1.1. Der Benutzername

Von der Sicht des Systems aus, ist der Benutzername die Antwort auf die Frage "Wer bist Du?" Als solches haben Benutzernamen eine wesentliche Bedingung zu erfüllen — sie müssen einzigartig sein. In anderen Worten muss jeder Benutzer einen Benutzernamen besitzen, der sich von allen anderen Benutzernamen im System unterscheidet.

Daher ist es unerlässlich — im vorhinein — festzulegen, wie Benutzernamen erzeugt werden sollen. Ansonsten finden Sie sich selbst in einer Position wieder, in der Sie gezwungen sind einzugreifen, wann immer ein neuer Benutzer einen Account anfordert.

Was Sie benötigen ist eine Namenskonvention für Benutzer-Accounts.

6.1.1.1. Namenskonventionen

Durch die Erstellung einer Namenskonvention für Benutzernamen können Sie sich selbst jede Menge an Problemen ersparen. Anstatt sich immer wieder neue Namen ausdenken zu müssen (und es für Sie immer schwieriger wird einen vernünftigen Namen zu erfinden), investieren Sie lieber etwas Arbeit im Voraus und entwickeln eine Konvention, welche bei der Erstellung aller nachfolgenden Benutzer-Accounts verwendet wird. Ihre Namenskonvention sollte möglichst einfach aufgebaut sein,

da ansonsten die Beschreibung selbst bei der Dokumentation einige Seiten in Anspruch nehmen könnte.

Die genaue Eigenschaft Ihrer Namenskonvention sollte etliche Faktoren berücksichtigen:

- Die Größe Ihres Unternehmens
- Die Struktur Ihres Unternehmens
- Die Beschaffenheit Ihres Unternehmens

Die Größe Ihres Unternehmens spielt eine entscheidende Rolle, da es letztendlich darauf hinweist, wie viele Benutzer von der Namenskonvention in Betracht gezogen werden müssen. Eine sehr kleines Unternehmen ist zum Beispiel in der Lage jeden Benutzer, dessen oder deren Vorname benutzen zu lassen. Für eine wesentlich grösseres Unternehmen wäre dies jedoch nicht möglich.

Die Struktur eines Unternehmens kann ebenso Auswirkungen auf die geeignetste Namenskonvention haben. Für Unternehmen mit einer sehr strikt festgelegten Struktur mag es angemessen sein, gewisse Elemente zu inkludieren, welche die Struktur wiederspiegeln. Zum Beispiel könnten Sie die Abteilungscodes als Teil jedes Benutzernamens integrieren.

Das allgemeine Wesen Ihres Unternehmens bringt ebenso mit sich, dass einige Namenskonventionen angebrachter sind als Andere. Ein Unternehmen, welches mit höchst klassifizierten Daten zu tun hat, mag sich für eine Namenskonvention entscheiden, welche von sämtlichen Aspekten einer persönlichen Identifikation, wie zum Beispiel durch den Namen, absieht. In einem solchen Unternehmen würde Maggie McOrmies Benutzername zum Beispiel LUH3417 lauten.

Hier finden Sie einige Namenskonventionen, welche andere Unternehmen bereits benutzt haben:

- Vorname (john, paul, george, usw.)
- Nachname (smith, jones, brown, usw.)
- Erste Initiale, gefolt vom Nachnamen (jsmith, pjones, gbrown, usw.)
- Nachname, gefolt vom Abteilungscode (smith029, jones454, brown191, usw.)

Tipp

Beachten Sie bitte, dass Namenskonventionen, welche verschiedene Daten zusammenfügen, um einen Benutzernamen zu erstellen, eventuell auch anstößige, beleidigende oder humorvolle Resultate erbringen. Deshalb empfehlen wir auch im Falle eines automatisierten Prozesses eine Art Nachprüfungsprozess zur Verfügung zu haben.

Die hier angeführten Namenskonventionen haben jedoch eines gemeinsam, nämlich die Möglichkeit, dass laut Namenskonvention an zwei Individuen eventuell der selbe Benutzername vergeben werden sollte. Dieses Phänomen wird auch als *Kollision* bezeichnet. Da jeder Benutzername einzigartig sein muss, ist es notwendig sich mit dem Thema Kollision zu beschäftigen. Im folgenden Abschnitt wird dieses Thema behandelt.

6.1.1.1.1. Kollisionen behandeln

Kollisionen sind beinahe unvermeidlich — egal wie sehr Sie auch versuchen dies zu vermeiden, Sie werden höchstwahrscheinlich früher oder später mit einer Kollision zu tun haben. Daher müssen Sie Kollisionen in Ihrer Namenskonvention einplanen. Es gibt verschiedenste Wege dies zu tun:

- Indem Sie aufeinanderfolgende Nummern an den kollidierenden Benutzernamen anhängen (smith, smith1, smith2, usw.)

- Indem Sie benutzerspezifische Daten an den kollidierenden Benutzernamen anhängen (smith, esmith, eksmith, usw.)
- Indem Sie unternehmensbezogene Informationen an den kollidierenden Benutzernamen anhängen (smith, smith029, smith454, usw.)

Methoden zu entwickeln, um Kollisionsprobleme lösen zu können, ist ein wichtiger Bestandteil jeder Namenskonvention. Jedoch wird es dadurch auch schwieriger für einen Außenstehenden einen Benutzernamen genauestens festzulegen. Daher ist der Nachteil der meisten Namenskonventionen, dass es mit höchster Wahrscheinlichkeit hin und wieder zu falsch adressierten e-Mails kommen kann.

6.1.1.2. Namensänderungen behandeln

Im Falle, dass Ihr Unternehmen eine Namenskonvention benutzt, welche auf dem Namen jedes einzelnen Benutzers basiert, ist es nahezu unumgänglich, dass Sie von Zeit zu Zeit mit einer Namensänderung zu tun haben. Auch wenn der eigentliche Name einer Person sich nicht ändert, so kann es zeitweise zu einer Anfrage kommen. Die Gründe dafür reichen von der Tatsache, dass Benutzer schlichtweg mit Ihrem Benutzernamen nicht zufrieden sind bis hin zu Benutzern, die je nach deren Stellung im Unternehmen um einen "angemesseneren" Benutzernamen ansuchen.

Ungeachtet der Begründung für eine Namensänderung, gibt es mehrere Punkte, die dabei beachtet werden müssen:

- Machen Sie die Änderung in *allen* betroffenen Systemen
- Die zugrundeliegende Benutzeridentifikation sollte immer konstant beibehalten werden
- Ändern Sie die Eigentumsrechte aller Dateien oder andere benutzerspezifische Ressourcen (wenn notwendig)
- E-Mail-bedingte Fragen behandeln

Zuallererst ist es wichtig sicherzugehen, dass der neue Benutzername auf allen Systemen verbreitet wird, auf denen der alte Benutzername in Gebrauch war. Ansonsten funktionieren Betriebssystemfunktionen, welche auf den Benutzernamen angewiesen sind lediglich auf einigen der Systeme und nicht auf allen Systemen. Bestimmte Betriebssysteme benutzen Zugriffskontrolle-Techniken, basierend auf Benutzernamen. Speziell diese Art von Systemen ist sehr anfällig für Probleme, die durch die Änderung von Benutzernamen entstehen.

Viele Betriebssysteme benutzen eine Art Benutzer-Identifikationsnummer für den Großteil der benutzerspezifischen Ablaufsteuerung. Um die Probleme bei Benutzernamensänderungen zu minimieren, empfehlen wir Ihnen falls möglich diese Identifikationsnummer beim alten sowie auch beim neuen Benutzernamen beizubehalten. Ansonsten kann dies zu einem Szenario führen, worin der Benutzer auf seine zuvor benutzen Dateien oder auf andere Ressourcen nicht mehr zugreifen kann.

Wenn die Benutzeridentifikationsnummer geändert werden muss, so ist es notwendig auch die Eigentumsberechtigung für sämtliche Dateien und benutzerbezogene Ressourcen zu ändern, um die neue Benutzeridentifikation widerzuspiegeln. Dies ist ein fehleranfälliger Vorgang, da es immer irgendetwas in einer vergessenen Ecke im System zu geben scheint, was im Endeffekt übersehen wird.

E-Mail-bezogene Themen sind wahrscheinlich der Bereich, in welchem sich die Änderung des Benutzernamens am schwierigsten gestaltet. Der Grund dafür ist folgender: Solange keine Schritte unternommen werden, dem entgegenzuwirken, werden an den alten Benutzernamen adressierte e-Mails nicht an den neuen Benutzernamen ergehen.

Unglücklicherweise, sind die Themen rund um e-Mail und die Änderung des Benutzernamens multidimensional. Einfach ausgedrückt, bedeutet eine Benutzernamensänderung, dass Dritte den korrekten Benutzernamen nicht mehr länger wissen können. Auf den ersten Blick mag dies nicht als ernstzunehmendes Problem erscheinen — wir empfehlen jedoch, dass Sie jeden in Ihrem Unternehmen

umgehend davon verständigen. Aber was passiert nun mit jemandem Außenstehenden, der dieses persönliche e-Mail geschickt hat? Wie können diese davon verständigt werden? Und was passiert mit den Mailing-Listen (internen und externen Ursprungs)? Wie können diese aktualisiert werden?

Es gibt keine einfache Antwort auf diese Fragen. Die beste Antwort darauf ist wahrscheinlich einen e-Mail-Alias anzulegen, sodass alle e-Mails, die an die alte Benutzeradresse adressiert sind automatisch an die neue Adresse weitergeleitet werden. Der Benutzer kann sodann dazu gedrängt werden, alle Absender von der Änderung zu benachrichtigen. Mit der Zeit werden immer weniger e-Mails mittels Alias eingehen. Letztendlich kann der Alias auch völlig entfernt werden.

Trotz der Tatsache, dass die Benutzung von einem Alias zu falschen Schlussfolgerungen führen kann (z.B. der Benutzer, welcher als esmith bekannt ist, ist auch gleichzeit noch immer als ejones bekannt), ist dies der einzige Weg um zu garantieren, dass e-Mails die richtige Person erreichen.

Wichtig

Sollte Sie e-Mail-Aliase benutzen, so gehen Sie sicher, dass alle notwendigen Schritte unternommen werden, um den alten Benutzernamen vor potenzieller Wiederbenutzung zu schützen. Sollten Sie das nicht tun und eine neuer Benutzer erhält Ihren alten Benutzernamen, so kann es zu Unterbrechungen in der e-Mail-Zustellung kommen (entweder für den Originalbenutzer oder auch den neuen Benutzer). Die genaue Art und Weise in der diese Unterbrechungen auftreten können, hängt selbstverständlich von der Art ab, wie die e-Mail-Zustellung in Ihrem System implementiert worden ist. Die zwei häufigsten Varianten sind:

- Der neue Benutzer erhält niemals e-Mails — alle werden an den Originalbenutzer vermittelt.
- Der Originalbenutzer bekommt plötzlich keine e-Mails mehr — alle werden an den neuen Benutzer vermittelt.

6.1.2. Passwörter

Wenn der Benutzername die Antwort auf die Frage "Wer bist Du?" darstellt, so ist das Passwort die Antwort auf die Aufforderung, die unweigerlich folgt:

"Beweise es!"

Eine fachlichere Umschreibung ist, dass ein Passwort ein Hilfsmittel darstellt, um die Authentizität einer Person zu bestätigen, welche sich als rechtmäßiger Benutzer mittels dem Benutzernamen ausgibt. Die Effektivität eines Passwort-basierten Authentifizierungsschemas stützt sich auf einige unterschiedliche Aspekte des Passwortes:

- Die Geheimhaltung des Passwortes
- Die Beständigkeit des Passwortes gegenüber dem Versuch es zu erraten
- Die Beständigkeit des Passwortes gegenüber einem Gewaltsakt in Form einer Attacke.

Passwörter, welche in ausreichender Form diese Punkte ansprechen, werden als *stark* bezeichnet, wohingegen diejenigen, die einen oder mehrer Punkte oder Risiken nicht ansprechen, als *schwach* bezeichnet werden. Starke Passwörter zu erstellen ist wichtig für die Sicherheit des gesamten Unternehmens, da diese mit einer geringeren Wahrscheinlichkeit herausgefunden oder erraten werden können. Es gibt zwei Möglichkeiten, um die Benutzung von starken Passwörtern durchzusetzen:

- Der Systemadministrator kann Passwörter für alle Benutzer erstellen.

- Der Systemadministrator kann die Benutzer selbst deren Passwörter erstellen lassen, wobei er gleichzeitig überprüft, ob die Passwörter akzeptabel stark sind.

Passwörter für alle Benutzer zu erstellen, stellt zwar sicher, dass diese starke Passwörter sind, kann aber zu einer beängstigenden Aufgabe werden, in Hinsicht auf das stetige Wachstum eines Unternehmens. Es beinhaltet ebenso ein höheres Risiko, dass Benutzer Ihre Passwörter niederschreiben.

Aus diesen Gründen bevorzugen die meisten Systemadministratoren, dass deren Benutzer selbst deren Passwörter erstellen. Ein guter Systemadministrator leitet jedoch immer Schritte ein, sich davon zu überzeugen, dass es sich dabei um starke Passwörter handelt.

Für Richtlinien zur Erstellung starker Passwörter, siehe Kapitel *Arbeitsplatz Sicherheit* in dem *Red Hat Enterprise Linux Sicherheitshandbuch*.

Die Notwendigkeit Passwörter unter allen Umständen geheim zu halten, sollte fest in der Denkweise eines jeden Systemadministrators verwurzelt sein. Jedoch geht dieser Punkt oft bei vielen Benutzern unter. Tatsache ist, dass viele Benutzer oft nicht einmal den Unterschied zwischen Benutzername und Passwort kennen. Dieser unglückliche Umstand bringt mit sich, dass ein gewisser Umfang an Benutzerweiterbildung unerlässlich ist, sodass Benutzern klar wird, dass deren Passwort so geheim gehalten werden muss, wie deren Gehaltsscheck.

Passwörter sollen so schwer als möglich zu erraten sein. Ein starkes Passwort ist dadurch gekennzeichnet, dass niemand jemals in der Lage ist es zu erraten, sogar wenn diese Person den Benutzer gut kennt.

Ein Gewaltsakt oder sogenannte Attacke auf ein Passwort hat den methodischen Versuch (normalerweise mittels einem Programm, das als *Password-Cracker* bekannt ist) jede mögliche Kombination von Passwörtern auszuprobieren zur Folge, in der Hoffnung, dass eventuell das korrekte Passwort gefunden wird. Ein starkes Passwort sollte so konstruiert werden, dass die Anzahl der potenziellen Passwörter, welche durchgetestet werden müssen, zur Folge haben, dass es einen möglichst langen Zeitraum in Anspruch nimmt, um nach dem Passwort zu suchen.

Starke und schwache Passwörter werden in den folgenden Abschnitten detaillierter behandelt.

6.1.2.1. Schwache Passwörter

Wie bereits erwähnt, besteht ein schwaches Passwort einen der folgenden drei Test nicht:

- Es ist geheim
- Es kann nicht erraten werden
- Es hält jedem Gewaltsakt in Form einer Attacke stand

Die folgenden Abschnitte behandelt die Schwachstellen von Passwörtern.

6.1.2.1.1. Kurze Passwörter

Ein kurzes Passwort ist gleichzeitig ein schwaches Passwort, da es einer Attacke weniger gut standhalten kann. Um dies zu demonstrieren, beachten Sie bitte folgende Tabelle, welche die Anzahl der potenziellen Passwörter zeigt, die im Falle einer Attacke durchgetestet werden müssten. (Es wird hierbei angenommen, dass die Passwörter lediglich aus Kleinbuchstaben bestehen.)

Passwortlänge	Potenzielle Passwörter
1	26
2	676
3	17.576

Passwortlänge	Potenzielle Passwörter
4	456.976
5	11.881.376
6	308.915.776

Tabelle 6-1. Passwortlänge versus der Nummer von potenziellen Passwörtern

Wie Sie sehen können, so steigt die Nummer der möglichen Passwörter dramatisch mit der Länge des Passwortes an.

Anmerkung

Auch wenn diese Tabelle bei sechs Zeichen endet, sollte dies nicht fälschlicherweise als Empfehlung aufgefasst werden, dass sechsstellige Passwörter lange genug sind, um ausreichende Sicherheit zu bieten. Generell gilt, je länger das Passwort, umso besser.

6.1.2.1.2. Limitierter Zeichensatz

Die Anzahl der verschiedenen Zeichen, aus denen ein Passwort bestehen kann, hat eine enorme Auswirkung auf die Möglichkeiten bei einer Attacke. Was wäre wenn wir zum Beispiel anstatt den 26 verschiedenen Zeichen, welche in einem Passwort in Kleinbuchstaben verwendet werden können, auch Zahlen verwenden? Dies würde bedeuten, dass jedes Zeichen in einem Passwort eines von 36 Zeichen, anstatt eines von nur 26 Zeichen sein könnte. Im Falle eines sechsstelligen Passwortes, steigt die Anzahl der Möglichkeiten von 308.915.776 auf 2.176.782.336.

Es geht noch weiter. Wenn wir nämlich alphanumerische Passwörter in Verbindung mit Groß- und Kleinschreibung (für diejenigen Betriebssysteme, die dies unterstützen) verwenden, so resultiert daraus eine Anzahl von 56.800.235.584 Möglichkeiten. Das Hinzufügen weiterer Zeichen (wie zum Beispiel Interpunktionszeichen) erhöht nochmals die Anzahl der möglichen Passwörter, was eine Attacke wesentlich erwschwert.

Jedoch sollte man immer daran denken, dass nicht jede Attacke auf ein Passwort eine Hacker-Attacke ist. Der folgende Abschnitt beschreibt weitere Merkmale eines schwachen Passwortes.

6.1.2.1.3. Erkennbare Wörter

Viele Attacken auf Passwörter basieren auf der Tatsache, dass Leute sich mit Passwörtern zufrieden geben, welche einfach zu merken sind. Deshalb sind die meisten Attacken Wörterbuch-basiert. In anderen Worten benutzt der Attacker verschiedene Wörterbücher mit dem Bestreben das Wort oder die Wörter zu finden, aus denen ein Passwort besteht.

Anmerkung

Viele Wörterbuch-basierte Programme zum Herausfinden des Passwortes benutzen Wörterbücher in mehreren Sprachen. Deshalb sollte Ihnen der Umstand, dass Sie ein nicht-deutsches oder auch nicht-englisches Passwort benutzt haben kein falsches Gefühl von Sicherheit vermitteln.

6.1.2.1.4. Persönliche Information

Passwörter, welche persönliche Informationen beinhalten (Name oder Geburtsdatum einer nahestehenden Person, eines Haustiers oder auch eine persönliche Identifikationsnummer) können bei einer Wörterbuch-basierten Attacke einfacher herausgefunden werden. Wenn jedoch ein sog. Attacker Sie persönlich kennt (oder auch ausreichend dazu motiviert ist Nachforschungen über Ihr Privatleben anzustellen), so könnte dieser/diese mit geringster Anstrengung auch Ihr Passwort erraten.

Zusätzlich zu Wörterbüchern inkludieren viele Passwort-Knacker auch gebräuchliche Namen, Daten oder andere derartige Informationen auf deren Suche nach dem richtigen Passwort. Deshalb könnte ein Attacker auch Ihr Passwort "meinhundbello" mit einem guten Passwort-Knacker herausfinden, ohne den Namen Ihres Hundes zu kennen.

6.1.2.1.5. Einfache Wortspiele

Das einfache Umdrehen der Reihenfolge von Zeichen in einem Passwort (jener Art, die zuvor ausgehend beschrieben worden ist), macht ein schwaches Passwort dadurch nicht stärker. Die meisten Passwort-Knacker tun dies bereits auch automatisch bei möglichen Passwörtern. Dies inkludiert auch das Ersetzen von bestimmten Buchstaben mit Zahlen in gebräuchlichen Wörtern. Hier sind einige Beispiele:

- drowssaPdaB1
- R3allyP00r

6.1.2.1.6. Das selbe Passwort für multiple Systeme

Auch wenn Sie ein starkes Passwort besitzen, so ist es nicht empfehlenswert, dieses Passwort auf mehr als einem System zu benutzen. Offenbar ist dies nicht möglich, wenn die Systeme derart konfiguriert sind, dass so etwas wie ein zentraler Authentifizierungsserver benutzt wird. In jedem anderen Fall sollten jedoch verschiedene Passwörter für jedes einzelen System benutzt werden.

6.1.2.1.7. Passwörter auf Papier

Ein anderer Weg aus einem starken Passwort ein Schwaches zu machen, ist es ganz einfach niederzuschreiben. Indem Sie ein Passwort auf Papier niederschreiben, haben Sie nicht mehr länger ein Geheimhaltungsproblem, sondern ein absolutes Sicherheitsproblem — jetzt müssen Sie diese Stück Papier sicher verwahren. Deshalb ist das Niederschreiben von Passwörtern niemals eine gute Idee.

Jedoch haben einige Unternehmen einen berechtigten Bedarf nach niedergeschriebenen Passwörtern. Zum Beispiel besitzen einige Unternehmen niedergeschriebene Passwörter als Teil der Vorgehensweise im Falle des Verlustes einer Schlüsselfigur unter den Angestellten (wie z.B. einem Systemadministrator). In diesem Fall wird die Niederschrift an einem physikalisch-sicheren Ort aufbewahrt, wobei es die Zusammenarbeit mehrerer Personen gleichzeit bedarf, um Zugang zu den Papieren zu bekommen. Dabei werden oft Tresorräume mit mehreren Schlössern und gesicherte Banksafe-Laden benutzt.

Jedes Unternehmen, welches diese Methode der Aufbewahrung von Passwörtern für Notfälle erkunden möchte, sollte sich darüber im Klaren sein, dass die reine Existenz einer Niederschrift ein weiteres Risiko-Element darstellt, egal wie sicher diese Passwörter auch aufbewahrt werden. Dies ist speziell der Fall, wenn generell bekannt ist, dass die Passwörter niedergeschrieben worden sind (und wo diese gelagert werden).

Unglücklicherweise sind niedergeschriebene Passwörter zumeist nicht als Teil eines Notfallplanes gedacht und daher auch nicht dementsprechend in einem Tresor verwahrt. Es handelt sich dabei zumeist um Passwörter für gewöhnliche Benutzer, welche in folgenden Plätzen untergebracht werden:

- In einer Schreibtischschublade (abgesperrt oder unverschlossen)
- Unter einem Keyboard
- In einer Brieftasche
- Auf die Seite des Bildschirms geklebt

Keine dieser Orte sind geeignete Plätze für ein niedergeschriebenes Passwort.

6.1.2.2. Starke Passwörter

Wir haben gesehen, was schwache Passwörter auszeichnet; die folgenden Abschnitte beschreiben die Merkmale, die alle starken Passwörter besitzen.

6.1.2.2.1. Längere Passwörter

Desto länger ein Passwort, desto weniger hoch ist die Chance, dass eine Attacke erfolgreich verläuft. Deshalb sollten Sie, falls vom System unterstützt, eine relativ grosse Anzahl von Mindestzeichen für das Passwort Ihrer Benutzer festlegen.

6.1.2.2.2. Erweiterter Zeichensatz

Fördern Sie die Benutzung von alphanumerischen Passwörtern, die aus Groß- und Kleinbuchstaben bestehen und bestehen Sie auf die Verwendung von zumindest einem nicht-alphanumerischen Zeichen bei allen Passwörtern:

- t1Te-Bf,te
- Lb@lbhom

6.1.2.2.3. Erinnerungswert

Ein Passwort ist nur dann stark, wenn man sich auch daran erinnern kann. Jedoch liegen 'einfach zu merken' und 'leicht zu erraten' oft sehr nahe beeinander. Geben Sie deshalb Ihren Benutzern einige Tipps, wie man erinnerungswerte Passwörter erstellt, die aber andererseit nicht einfach zu erraten sind.

Wenn Sie zum Beispiel einen bekannten Spruch oder eine bekannte Phrase nehmen und lediglich die ersten Buchstaben jeden einzelnen Wortes als Ausgangspunkt für Ihr Passwort wählen. Das Resultat ist erinnerungswert (weil der Spruch selbst, auf dem es basiert erinnerungswert ist) und doch das Resultat kein Wort beinhaltet oder darstellt.

Anmerkung

Beachten Sie dabei jedoch, dass lediglich das Benutzen der ersten Buchstabens eines jeden Wortes nicht ausreichend sind, um ein starkes Passwort zu erzeugen. Sorgen Sie immer dafür, den Passwortzeichensatz zu erhöhen, indem Sie alphanumerische Zeichen, Groß- und Kleinschreibung sowie ebenfalls zusätzlich Spezialzeichen verwenden.

6.1.2.3. Passwort Fälligkeit

Falls möglich, empfehlen wir Passwort-Fälligkeitsdaten in Ihrem Unternehmen einzuführen. Passwort-Fälligkeit ist ein Merkmal (in Zusammenhang mit vielen Betriebssystemen erhältlich), welches ein Zeitlimit aufstellt, bis zu dem das jeweilige Passwort als gültig angesehen ist. Am Ende der Gültigkeitsdauer eines Passwortes, wird der Benutzer mittels Bedienerhinweis dazu aufgefordert ein neues Passwort einzugeben, welches sodann bis zu dessen neuem Ablaufdatum benutzt werden kann.

Für die meisen Systemadminsitratoren ist die Hauptfrage zum Thema Passwort-Fälligkeit diejenige, nach der Gültigkeitsdauer eines Passwortes.

Es gibt zwei völlig entgegengesetzte Punkte, die im Bezug auf Passwort-Gültigkeitsdauer zu beachten sind:

- Benutzerkomfort
- Sicherheit

Übertrieben ausgedrückt, würde eine Passwort-Gültigkeitsdauer von 99 Jahren sehr wenig Unannehmlichkeiten (wenn überhaupt) beim Benutzer hervorrufen. Jedoch würde es wenig (oder gar nicht) zum Thema Sicherheit beitragen.

Ebenso übertrieben ausgedrückt, würde eine Passwort-Gültigkeitsdauer von 99 Minuten sehr große Unannehmlichkeiten für den Benutzer hervorrufen. Der Sicherheitsfaktor wäre dadurch jedoch ausserordentlich hoch.

Es geht hauptsächlich darum, ein Mittelmaß zwischen dem Bestreben nach Bequemlichkeit für alle Benutzer und der Erfordernis nach höchster Sicherheit für das Unternehmen zu finden. Für die meisten Unternehmen befindet sich die allgemeinübliche Passwort-Lebensdauer im Wochen- oder Monatsbereich.

6.1.3. Zugriffskontrolle Information

Zusammen mit Benutzername und Passwort, beinhalten Benutzer-Accounts ebenso Informationen zum Thema Zugriffskontrolle. Diese Information kann verschiedene Formen je nach Art des verwendeten Betriebssystemes annehmen. Jedoch beinhalten diese Arten von Informationen zumeist:

- Systemweite benutzerspezifische Identifikation
- Systemweite gruppenspezifische Identifikation
- Listen von zusätzlichen Gruppen/Leistungsmerkmalen, denen ein Benutzer zugeordnet ist
- Standardisierte Zugriffsinformation, welche auf alle vom Benutzer erstellten Dateien und Ressourcen zutrifft

In einigen Unternehmen ist es niemals notwendig, auf die Zugriffskontrollinformation eines Benutzers zuzugreifen. Dies trifft vor allem auf eigenständige, persönliche Arbeitsplatzsysteme zu. Für andere Unternehmen, speziell diejenigen, die Gebrauch von netzwerkweitem Resource-Sharing zwischen verschiedenen Benutzergruppen machen, besteht die Notwendigkeit, dass Zugriffskontrollinformationen der Benutzer weitgehend modifiziert werden.

Das Arbeitspensum, welches dazu benötigt wird, um die Zugriffskontrollinformation Ihrer Benutzer zu warten, variiert gemäß dem Nutzungsgrad der Zugriffskontrollfeatures des Betriebssystemes Ihrer Organisation. Einerseits ist es nicht schlecht, in hohem Maße auf diese Merkmale angewiesen zu sein (Tatsache ist, dass es eventuell unvermeidlich ist), andererseits bedeutet dies jedoch, dass Ihre Systemumgebung mehr Aufwand im Bereich der Wartung erfordert und dass jeder Benutzer-Account anfälliger für Miskonfigurationen ist.

Im Falle, dass Ihr Unternehmen diese Art von Umgebung benötigt, sollten Sie daher die genauen Schritte, welche zur Erstellung und Konfiguration eines Benutzer-Accounts notwendig sind, dokumentieren. Tatsächlich sollten Sie im Falle von verschiedenen Arten von Benuzer-Accounts jeden einzelnen Account dokumentieren (Erstellung eines neuen Finanz-Benutzer-Accounts, eines neuen Operations-Benutzer-Accounts, usw.).

6.1.4. Accounts und Ressourcen-Zugang tagtäglich verwalten

Wie ein altes Sprichwort so schön sagt, ist die einzige Konstante im Leben die Veränderung. Dies trifft auch auf den Umgang mit Ihrer Benutzerschaft zu. Leute kommen und gehen oder wechseln deren Verantwortungsbereich. Deshalb müssen Systemadministratoren in der Lage sein, auf diese tagtäglich normal vorkommenden Veränderungen in deren Unternehmen zu reagieren.

6.1.4.1. Neuzugänge

Wenn ein neues Mitglied Ihrem Unternehmen beitritt, so wird diesen mormalerweise Zugang zu verschiedenen Ressourcen (abhängig von deren Verantwortungsbereich) gewährt. Diese bekommen wahrscheinlich einen Arbeitsplatz zugewiesen, ein Telefon und einen Schlüssel für die Eingangstür.

Diese bekommen wahrscheinlich auch Zugang zu einem oder mehreren Computern in Ihrem Unternehmen. Als Systemadministrator liegt es in Ihrem Verantwortungsbereich sicherzustellen, dass die umgehend und entsprechend durchgeführt wird. Wie sollten Sie vorgehen?

Bevor Sie irgendetwas tun können, müssen Sie zunächst einmal von der Ankunft der neuen Person informiert sein. Dies wird in verschiedenen Unternehmen ganz unterschiedlich gehandhabt. Hier sind einige Möglichkeiten:

- Schaffen Sie einen Prozess, bei welchem die Personalabteilung Ihres Unternehmens Sie von der Ankunft einer neuen Person verständigt.
- Erstellen Sie ein Formular, welches vom Vorgesetzten dieser Person ausgefüllt und dazu benutzt werden kann, um einen Benutzer-Account anzufordern.

Veschiedene Unternehmen erfordern verschiedene Vorgehensweisen. Schlussendlich ist es unerlässlich einen höchst-verlässlichen Prozess an der Hand zu haben, der Sie darauf hinweist, sobald accountbezogene Arbeit erledigt werden muss.

6.1.4.2. Kündigungen

Tatsache ist, dass Personen Ihr Unternehmen auch verlassen werden. Manchmal geschieht dies unter glücklichen und ein anderes mal unter weniger glücklichen Umständen. In jedem Fall ist es notwendig, dass Sie über diese Situation bestens informiert sind, sodass Sie die notwendigen Schritte einleiten können.

Zumindest sollten die angemessenen Schritte folgendes beinhalten:

- Den Zugang des Benutzers zu allen Systemen und dazugehörigen Ressourcen sperren (normalerweise mittels Änderung/Sperrung des Benutzerpasswortes)
- Eine Sicherungskopie der Benutzerdateien erstellen, für den Fall, dass diese etwas beinhalten, das zu einem späteren Zeitpunkt benötigt wird
- Den Zugang zu Dateien des Benutzers koordinieren

Die höchste Priorität ist das System gegen einen gerade ausgeschiedenen Benutzer abzusichern. Dies ist besonders von Bedeutung, wenn der Benutzer unter Umständen entlassen worden ist, was beim Benutzer böswillige Absichten gegenüber dem Unternehmen hervorrufen könnte. Jedoch ist es auch

unter anderen gegebenen Umständen im besten Interesse des Unternehmens rasch und verlässlich den entsprechenden Zugang zum System zu sperren.

Dies weist darauf hin, dass auch hier ein Prozess zur Ihrer Alarmierung in Hinsicht auf Entlassungen im Unternehmen eingeführt werden muss — bevorzugterweise sogar bevor die Kündigung stattgefunden hat. Dies setzt natürlich voraus, dass Sie eng mit der Personalabteilung Ihres Unternehmens zusammenarbeiten, um sicherzustellen, dass Sie rechtzeitig von Kündigungen informiert werden.

Tipp

Im Umgang mit sogenannten "lock-downs" als Folge von Kündigungen, ist genauestes Timing wichtig. Wird die Sperrung erst nach der eigentlichen Kündigung durchgeführt, so besteht die Gefahr, dass die gerade gekündigte Person sich unerlaubterweise nochmals Zugang zum System verschafft. Wenn die Sperrung jedoch stattfindet bevor die jeweilige Kündigung ausgesprochen worden ist, so könnte die betreffende Person zu früh alarmiert werden und der gesamte Prozess dadurch für alle Beteiligten erschwert werden.

Die Kündigung wird zumeist mit einem Meeting zwischen der zu kündigenden Person und deren Manager sowie einem Vertreter der Personalabteilung Ihres Unternehmens eingeleitet. Deshalb würde ein Prozess, bei dem Sie genau am Beginn dieser Besprechung alarmiert werden, sicherstellen, dass der Vorgang der Sperrung zeitgerecht erfolgt.

Sobald der Zugang gesperrt worden ist, ist es Zeit eine Sicherungskopie der Dateien der gerade entlassenen Person durchzuführen. Diese Sicherungskopie kann Teil des Standard-Backups des Unternehms sein oder auch eine Sicherungsprozedur, welche lediglich der Sicherung von alten und hinfälligen Benutzer-Accounts dient. Punkte, wie zum Beispiel Datenaufbewahrungs-Regulationen, die Konservierung von Daten im Falle eines Gerichtsverfahrens wegen ungerechtfertigter Kündigung und dergleichen spielen alle ein wichtige Rolle in der Findung der geeignetsten Art, Sicherungskopien zu erstellen.

In jedem Fall ist eine sofortige Sicherungskopie empfehlenswert, da der nächste Schritt (Zugang des Managers zu den Dateien der gerade entlassenen Person) die unbeabsichtigte Löschung von Daten zur Folge haben könnte. Unter solchen Umständen ermöglicht eine aktuelle Sicherungskopie die einfache Wiederherstellung von Daten, was den gesamten Ablauf nicht nur seitens des Managers, sondern auch Ihrerseits einfacher gestaltet.

An diesem Punkt müssen Sie festlegen, welchen Zugang zu den entsprechenden Dateien der Manager, der gerade entlassenen Person, benötigt. Abhängig von Ihrem Unternehmen und dem Zuständigkeitsbereich derjenigen Person, kann entweder kein Zugang benötigt werden oder auch der vollständige Zugang zu allen Daten.

Im Falle, dass die Person das System für mehr als hin und wieder ein zufälliges e-Mail benutzt hat, ist es höchstwahrscheinlich, dass der Manager sich kurz die Dateien durchsieht, um festzustellen was behalten werden muss und was verworfen werden kann. Bei Abschluss dieses Prozesses können zumindest einige der Dateien an den Nachfolger oder die Nachfolgerin der entlassenen Person weitergegeben werden. Ihre Unterstützung wird eventuell in diesem letzten Abschnitt des Prozesses benötigt werden, sofern der Manager selbst nicht in der Lage ist, dies selbst durchzuführen. Dabei kommt es selbstverständlich auf die Dateien und die Art der Arbeit an, welche von Ihrem Unternehmen durchgeführt wird.

6.1.4.3. Berufswechsel

Auf die Anfrage zur Erstellung neuer Benutzer-Accounts zu reagieren und die Abfolge von Tätigkeiten einzuhalten, welche notwendig sind, um einen Account in Zusammenhang mit der Kündigung einer Person zu schließen, sind beides relativ unkomplizierte Vorgänge. Jedoch ist es nicht so klar definiert, wenn sich der Aufgabenbereich einer Person innerhalb des Unternehmens verändert. Manchmal sind Änderungen des Benutzer-Accounts notwendig und manchmal auch hinfällig.

Zumindest drei Personen sind dabei involviert, wenn es darum geht sicherzustellen, dass der Benutzer-Account angemessen rekonfiguriert wird und dem neuen Aufgabenbereich derjenigen Person entspricht:

- Sie
- Der vorhergende Manager des Benutzers
- Der neue Manager des Benutzers

Es sollte möglich sein, dass alle drei Personen (Sie selbst miteingeschlossen) festlegen können, was einerseits getan werden muss, um klar den alten Verantwortungsbereich auszugliedern und was andererseits notwendig ist, um den Account auf die neuen Anforderungen vorzubereiten. In vieler Hinsicht kann diese Vorgehensweise auch gleichgesetzt werden mit dem Schließen und Neuerstellen eines Benutzer-Accounts. Tatsächlich wird dies von einigen Unternehmen derartig gehandhabt.

Jedoch ist es wahrscheinlicher, dass ein Benutzer-Account behalten und entsprechend den neuen Anforderungen und Aufgaben modifiziert wird. Diese Annäherung bedarf einer vorsichtigen Durchsicht des Accounts, um sicherzustellen, dass keine alten Ressourcen oder Zugriffsprivilegien auf dem Account zurückbleiben und dass der Account lediglich die Ressourcen und Privilegien passend zum neuen Aufgabenbereich des Benutzers besitzt.

Was die Situation noch weiters verkompliziert, ist die Tatsache, dass es oft eine sogennante Übergangsperiode gibt, in welcher der Benutzer Aufgaben erfüllt, die sowohl dem alten, als auch dem neuen Aufgabenbereich angehören. Hier kann Ihnen vom alten und neuen Manager geholfen werden, indem ein bestimmter Zeitrahmen für diese Übergangsperiode angegeben wird.

6.2. Verwaltung von Benutzer-Ressourcen

Benutzer-Accounts zu erstellen, ist nur ein Teil des Aufgabenbereiches eines Systemadminstrators. Die Verwaltung von Benutzer-Ressourcen ist ebenfalls ein essentieller Bestandteil. Deshalb müssen drei Punkte in Betracht gezogen werden:

- Wer auf gemeinsam genutzte Daten zugreifen kann
- Wo Benutzer auf diese Daten zugreifen können
- Welche Beschränkungen sind eingeräumt worden, um den Missbrauch von Ressourcen zu verhindern

Die folgenden Abschnitte behandeln kurz jedes dieser Themen.

6.2.1. Wer kann auf gemeinsam genutzte Daten zugreifen

Der Zugang eines Benutzers zu einer Applikation, einer Datei oder einem Verzeichnis wird von den Berechtigungen bestimmt, die in Bezug auf diese Applikation, diese Datei oder dieses Verzeichnis Anwendung finden.

Zusätzlich ist es oft hilfreich, wenn verschiedene Berechtigungen für verschiedene Benutzerklassen Anwendung finden. Zum Beispiel sollte ein gemeinsam benutzter temporärer Speicher in der Lage sein, die unbeabsichtigte (oder auch böswillige) Löschung der Datei eines Benutzers durch alle anderen Benutzer zu verhindern, wobei dem Besitzer der Datei trotzdem voller Zugang gewährt wird.

Ein weiteres Beispiel ist die Zugriffsberechtigung zum Heimverzeichnis eines Benutzers. Nur der Besitzer des jeweiligen Heimverzeichnisses sollte in der Lage sein hierbei Dateien zu erstellen oder einzusehen. Allen anderen Benutzern sollte der Zugang verweigert werden (ausser der Benutzer gibt dazu seine Einwilligung). Dies erhöht den persönlichen Datenschutz des jeweiligen Benutzers und verhindert die mögliche Unterschlagung von persönlichen Dateien.

Es gibt jedoch viele Situationen, in denen mehrere Benutzer Zugang zu den selben Ressourcen auf einem Rechner benötigen. In diesem Fall ist eine vorsichtige Erstellung von gemeinsamen Gruppen eventuell notwendig.

6.2.1.1. Gemeinsame Gruppen und Daten

Wie in der Einleitung bereits erwähnt, sind Gruppen logische Konstruktionen, welche dazu benutzt werden können, Accounts für spezielle Zwecke in Cluster zu verpacken.

Wenn Benutzer innerhalb eines Unternehmens verwaltet werden, ist es ratsam festzulegen, auf welche Daten von gewissen Abteilungen zugegriffen werden kann, auf welche Daten von anderen nicht zugegriffen werden sollte und welche Daten von allen benutzt werden sollten. Dies genauestens festzulegen ist höchsthilfreich in der Erstellung einer passenden Gruppenstruktur, gemeinsam mit den entsprechenden Rechten auf die gemeinsamen Daten.

Nehmen Sie zum Beispiel an, dass die Abteilung zur Einbringung von Außenständen eine Liste aller Konten führen muss, welche rückständig in deren Zahlungen sind. Diese müssen jene Liste auch gemeinsam mit der Inkassoabteilung benutzen können. Wenn beide Abteilungen zu Mitgliedern einer Gruppe genannt `Accounts` gemacht werden, so kann diese Information in einem gemeinsamen Verzeichnis abgelegt werden (welches der `Accounts`-Gruppe angehört), welches eine Gruppen-Lese-/Schreibberechtigung auf dieses Verzeichnis besitzt.

6.2.1.2. Gruppenstruktur festlegen

Einige der Herausforderungen, mit denen Systemadministratoren bei der Erstellung von gemeinsamen Gruppen konfrontiert sind:

- Welche Gruppen sind zu erstellen
- Wer wird einer bestimmten Gruppe zugeordnet
- Welche Art von Berechtigungen sollten diese gemeinsamen Ressourcen besitzen

Eine vernünftige Vorgehensweise ist dabei von Nutzen. Eine Möglichkeit ist das Widerspiegeln der Unternehmensstruktur bei der Erstellung von Gruppen. Zum Beispiel, wenn es eine Finanzabteilung gibt, erstellen Sie ein Gruppe genannt `Finanzen` und machen alle Mitglieder dieser Abteilung zu Mitgliedern dieser Gruppe. Sollten die Finanzinformationen zu heikel für den Einblick durch das gesamte Unternehmen, jedoch von höchster Wichtigkeit für Vorgesetzte innerhalb der Organisation sein, so erteilen Sie allen Vorgesetzen Gruppen-Level-Berechtigungen auf alle Verzeichnisse und Daten zuzugreifen, welche von der Finanzabteilung genutzt werden, indem Sie alle Vorgesetzten zur `Finanz`-Gruppe hinzufügen.

Es hat sich auch bewährt auf Nummer sicher zu gehen, wenn gewisse Berechtigungen an Benutzer vergeben werden. Auf diesem Weg ist es höchst unwahrscheinlich, dass heikle Informationen in die falschen Hände geraten.

Durch diese Vorgehensweise bei der Erstellung der Gruppenstruktur in Ihrem Unternehmen kann der Bedarf nach Zugriff auf gemeinsame Daten innerhalb des Unternehmens sicher und effektiv gedeckt werden.

6.2.2. Wo Benutzer auf gemeinsame Daten zugreifen

Wann immer Daten von verschiedenen Benutzern gemeinsam benutzt werden, ist es üblich einen zentralen Server (oder eine Gruppe von Servern) zu benutzen, welcher bestimmte Verzeichnisse für andere Rechner im Netzwerk zugänglich macht. Auf diese Art werden Daten an einem Ort gespeichert. Die Synchronisation von Daten zwischen mehreren Rechnern wird dadurch hinfällig.

Bevor Sie dementsprechend vorgehen, müssen Sie zuallererst festlegen, welche Systeme Zugriff auf die zentral gespeicherten Daten haben sollen. Dabei sollten Sie Notizen von den Betriebssystemen machen, die von den jeweiligen Systemen benutzt werden. Diese Information hat Einfluss auf Ihre Fähigkeit eine solche Vorgehensweise zu implementieren, da Ihr Speicherserver die Fähigkeit besitzen muss, dessen Daten an jedes einzelne Betriebssystem in Ihrem Unternehmen weitergeben zu können.

Unglücklicherweise können Konflikte bezüglich Datei-Eigentum auftreten, sobald Daten von mehreren Computern in einem Netzwerk gemeinsam benutzt werden.

6.2.2.1. Globale Eigentumsfragen

Es hat Vorteile, wenn Daten zentral gespeichert werden und auf diese von verschiedenen Rechnern im Netwerk zugegriffen werden kann. Stellen Sie sich jedoch für einen Moment vor, dass jeder dieser Rechner eine logisch-verwaltete Liste von Benutzer-Accounts besitzt. Was passiert, wenn die Liste der Benutzer auf jedem dieser Systeme nicht einheitlich mit der Liste von Benutzern auf dem zentralen Server ist? Oder sogar noch schlimmer: Was wäre wenn die Liste von Benutzern auf jedem einzelnen dieser Systeme nicht einmal miteinander übereinstimmen?

Vieles hängt davon ab, wie Benutzer und Zugriffsrechte in jedem System implementiert sind. In einigen Fällen ist es jedoch möglich, dass Benutzer A eines Systems eigentlich als Benutzer B auf einem anderen System bekannt ist. Dies kann zu einem richtigen Problem werden, wenn Daten innerhalb dieser Systeme gemeinsam benutzt werden. Daten, auf die von Benutzer A zugegriffen werden kann, können plötzlich ebenso von Benutzer B von einem anderen Systemgelesen werden.

Aus diesem Grund benutzen viele Unternehmen eine Art Benutzerdatenbank. Dies garantiert, dass Benutzerlisten sich auf verschiedenen Systemen nicht überschneiden.

6.2.2.2. Heimverzeichnisse

Ein weiteres Problem, mit dem sich Systemadministratoren auseinandersetzen müssen, ist die Frage, ob Benutzer zentral gespeicherte Heimverzeichnisse besitzen sollten.

Der hauptsächliche Vorteil zentralisierter Heimverzeichnisse auf einem netzwerkverbundenen Server liegt darin, dass ein Benutzer von jedem Rechner im Netzwerk aus auf seine Dateien in seinem Heimverzeichnis zugreifen kann.

Der Nachteil ist derjenige, dass wenn das Netzwerk ausfällt, sämtliche Benutzer nicht mehr auf deren Heimverzeichnisse und somit auf deren Dateien zugreifen können. In manchen Situationen (wie z.B. in Unternehmen, die vornehmlich Laptops verwenden) ist es nicht wünschenswert zentralisierte Heimverzeichnisse zu besitzen. Wenn es jedoch für Ihr Unternehmen sinnvoll erscheint, so kann der Einsatz von zentralisierten Heimverzeichnissen das Leben eines Systemadministrators um ein Vielfaches vereinfachen.

6.2.3. Welche Hemmnisse werden eingesetzt, um den Missbrauch von Ressourcen zu verhindern

Die vorsichtige Organisation von Gruppen und Zuteilung von Berechtigungen für gemeinsame Ressourcen ist eines der wichtigsten Aufgaben eines Systemadministrators, um den Missbrauch von Ressourcen innerhalb eines Unternehmens zu verhindern. Auf diese Art wird denjenigen der Zugang zu heiklen Ressourcen verweigert, die keinen Zugang dazu haben sollten.

Ganz egal wie Ihr Unternehmen diese Dinge angeht, der beste Schutz gegen den Missbrauch von Ressourcen ist immer noch fortwährende Wachsamkeit auf Seiten des Systemadministrators. Ihre Augen immer offen zu halten, ist oft der einzige Weg eine unangenehme Überraschung zu vermeiden.

6.3. Red Hat Enterprise Linux-Spezifische Informationen

Die folgenden Abschnitte beschreiben die verschiedenen für Red Hat Enterprise Linux spezifischen Merkmale, welche sich auf die Administration von Benutzer-Accounts und die dazugehörigen Ressourcen beziehen.

6.3.1. Benutzer-Accounts, Gruppen und Berechtigungen

Unter Red Hat Enterprise Linux kann ein Benutzer sich im System anmelden und jede beliebige Applikation oder Datei benutzen, zu welcher dieser eine Zugriffsberechtigung besitzt, nachdem ein regulärer Benutzter-Account erstellt worden ist. Red Hat Enterprise Linux bestimmt, ob ein Benutzer oder eine Gruppe auf diese Ressourcen gemäß den entsprechenden Berechtigungen zugreifen darf oder auch nicht.

Es gibt drei verschiedene Berechtigungen für Dateien, Verzeichnisse und Applikationen. Diese Berechtigungen werden dazu benutzt, die erlaubten Arten des Zugriffs zu kontrollieren. Verschiedene Symbole, bestehend aus einem Zeichen, werden dazu benutzt, um jede einzelne Berechtigung in einem Verzeichnis aufzulisten. Die folgenden Symbole werden dabei benutzt:

- `r` — kennzeichnet, dass Benutzer den Inhalt einer Datei anzeigen dürfen.
- `w` — kennzeichnet, dass Benutzer den Inhalt der Datei ändern dürfen.
- `x` — kennzeichnet, dass Benutzer Dateien ausführen dürfen, sofern dies eine ausführbare Datei oder ein Script ist.

Ein viertes Symbol (`-`) kennzeichnet, dass kein Zugang erlaubt ist.

Jede der drei Zugriffsberechtigungen wird drei verschiedenen Benutzer-Kategorien zugewiesen. Die Kategorien sind:

- *Eigentümer* — Der Eigentümer der Datei oder Applikation.
- *Gruppe* — Die Gruppe, welche die Datei oder Applikation besitzt.
- *Andere* — Alle Benutzer mit Zugang zum System.

Wie bereits zuvor erklärt, ist es möglich die Zugriffsberechtigungen für eine Datei einzusehen, indem man eine Auflistung in langem Format mit dem Befehl `ls -l` aufruft. Wenn zum Beispiel der Benutzer `juan` eine ausführbare Datei namens `foo`erzeugt, so würde das Ergebnis des Befehls `ls -l foo` wie folgt erscheinen:

```
-rwxrwxr-x    1 juan     juan            0 Sep 26 12:25 foo
```

Die Berechtigungen für diese Datei sind am Beginn der jeweiligen Zeile, beginnend mit `rwx` aufgelistet. Der erste Satz von Symbolen definiert den Benutzerzugang — in diesem Beispiel hat der Benutzer `juan` vollen Zugang und besitzt Lese-, Schreib- und Ausführberechtigung für diese Datei. Der nächste Satz von `rwx`-Symbolen definiert die Gruppenzugangsberechtigung (wieder mit vollem Zugang), wobei der letzte Satz von Symbolen die Zugangsberechtigungen für alle anderen Benutzer definiert. Hierbei ist allen anderen Benutzern erlaubt, die Datei zu lesen und auszuführen, jedoch nicht diese in irgendeiner Art zu verändern.

Was dabei im Auge behalten werden sollte, ist der wichtige Punkt, dass in Bezug auf Zugangsberechtigungen und Benutzer-Accounts jede Applikation auf Red Hat Enterprise Linux in Zusammenhang mit einem spezifischen Benutzer abläuft. Im Falle, dass Benutzer `juan` eine Applikation startet, bedeutet dies, dass die Applikation Benutzer `juan`s Kontext benutzt. In manchen Fällen kann es jedoch vorkommen, dass eine Applikation eine noch privilegiertere Zugansebene benötigt, um eine Aufgabe ausführen zu können. Zu dieser Art von Applikationen zählen zum Beispiel auch diejenigen, welche Systemeinstellungen bearbeiten oder Benutzer anmelden. Aus diesem Grund wurden spezielle Berechtigungen entworfen.

Hier finden Sie drei dieser speziellen Berechtigungen innerhalb von Red Hat Enterprise Linux Diese sind:

- *Setuid* — nur für Applikationen benutzt, gibt diese Berechtigung an, dass diese Applikation als Datei-Eigentümer ausgeführt werden muss und nicht als Benutzer, der diese Applikation ausführt. Dies wird durch das Symbol `s`, welches anstatt `x` steht, gekennzeichnet. Wenn der Besitzer der Datei keine Ausführberechtigung besitzt, so wird das `S` großgeschrieben, um diese Tatsache zu verdeutlichen.
- *Setgid* — hauptsächlich für Applikationen benutzt, gibt diese Berechtigung an, dass die Applikation als Gruppe ausgeführt werden muss, welche der Eigentümer der Datei ist und nicht als Gruppe des Benutzers, welcher die Applikation ausführt.

  Wenn in einem Verzeichnis eingesetzt, bedeutet dies, dass alle innerhalb des Verzeichnisses erstellten Dateien der Gruppe gehören, welche das Verzeichnis besitzt und nicht der Gruppe von Benutzern, welche die Datei erstellt hat. Die Setgid-Berechtigung wird durch das Symbol `s` anstatt `x` in der Gruppenkategorie angezeigt. Wenn der Gruppen-Eigentümer der Datei oder des Verzeichnisses keine Ausführberechtigung besitzt, so wird `S` großgeschrieben, um dies zu verdeutlichen.
- *Sticky Bit* — hauptsächlich auf Verzeichnissen benutzt, bestimmt dieses Bit, dass eine Datei, die in diesem Verzeichnis erstellt worden ist, lediglich vom Benutzer entfernt werden kann, welcher diese erstellt hat. Es wird durch das Symbol `t` anstatt `x` in der Andere-Kategorie angezeigt.

  Unter Red Hat Enterprise Linux wird das Sticky Bit genau aus diesem Grund standardmäßig bei dem `/tmp/`-Verzeichnis gesetzt.

6.3.1.1. Benutzernamen und UIDs, Gruppen und GIDs

In Red Hat Enterprise Linux dienen Benutzer-Account und Gruppen-Namen hauptsächlich dem Komfort von Personen. Intern benutzt das System numerische Identifizierungszeichen. Für Benutzer ist diese Identifizierung als *UID* bekannt, während für Gruppen diese Identifizierung als *GID* bekannt ist. Programme, welche Benutzer- oder Gruppeninformationen für Benutzer verfügbar machen, übersetzen die UID/GID-Werte in visuell-lesbare Gegenstücke.

Wichtig

UIDs und GIDs müssen weltweit einzigartig innerhalb Ihres Unternehmens sein, sollten Sie beabsichtigen Dateien und Ressourcen über ein Netzwerk gemeinsam zu benutzen. Ansonsten würden jegliche Zugangskontrollen scheitern, da diese auf UIDs und GIDs basieren und nicht auf Benutzer- und Gruppennamen.

Speziell im Falle, dass sich `/etc/passwd`- und `/etc/group`-Dateien auf einem Dateiserver und auf dem Arbeitsplatz eines Benutzers in Bezug auf die UIDs oder GIDs unterscheiden, so kann die ungenaue Verwendung von Berechtigungen Sicherheitsfragen aufwerfen.

Wenn zum Beispiel Benutzer `juan` eine UID von 500 auf einem Desktop-Computer besitzt, so werden Dateien, die `juan` auf einem Dateiserver erstellt, mit Benutzer UID 500 erzeugt. Wenn sich jedoch Benutzter `bob` lokal auf einem Dateiserver anmeldet (oder auch einem anderen Computer) und `bob`s Account auch eine UID von 500 besitzt, so hat `bob` vollen Zugang zu `juan`s Dateien und umgekehrt.

Deshalb müssen UID- und GID-Kollisionen mit allen Mitteln vermieden werden.

Es gibt zwei Fälle, in denen der eigentliche numerische Wert der UID oder GID eine spezifische Bedeutung hat. Eine UID und GID von Null (0) werden für den `root`-User benutzt und werden speziell behandelt von Red Hat Enterprise Linux — jeglicher Zugang wird automatisch gewährt.

Der zweite Fall ist der, dass UIDs und GIDs unter 500 für Systembenutzung reserviert sind. Zum Unterschied von UID/GID gleich Null (0) werden UIDs und GIDs unter 500 nicht speziell behandelt.

Jedoch dürfen diese UIDs/GIDs niemals einem Benutzer zugewiesen werden, da es sehr wahrscheinlich ist, dass eine Computerkomponente eine dieser Nummern benutzt oder irgendwann in der Zukunft benutzen wird. Für weitere Informationen zu diesen Standardbenutzern und -gruppen, siehe Kapitel *Benutzer und Gruppen* im *Red Hat Enterprise Linux Referenzhandbuch*.

Wenn neue Benutzer-Accounts mittels der Red Hat Enterprise Linux Standard-Tools zur Benutzer-Erstellung hinzugefügt werden, so wird dem neuen Benutzer-Account die erstmöglich erhältliche UID und GID beginnend mit 500 zugewiesen. Dem nächsten neuen Benutzer-Account wird sodann UID/GID 501 zugewiesen, gefolgt von UID/GID 502, usw..

Ein kurzer Überblick über die verschiedenen Benutzer-Erzeugungstools, welche unter Red Hat Enterprise Linux erhältlich sind, scheint später in diesem Kapitel auf. Jedoch bevor diese Tools besprochen werden, behandelt der nächste Abschnitt die Dateien, welche von Red Hat Enterprise Linux benutzt werden, um System-Accounts und -Gruppen zu definieren.

6.3.2. Dateien, die Benutzer-Accounts und -Gruppen kontrollieren

Auf Red Hat Enterprise Linux werden Informationen über Benutzer-Accounts und -Gruppen in mehreren Textdateien innerhalb des `/etc/`-Verzeichnisses gespeichert. Wenn ein Systemadministrator neue Benutzer-Accounts anlegt, müssen diese Dateien entweder manuell bearbeitet werden oder es müssen Applikationen benutzt werden, um die notwendigen Änderungen durchzuführen.

Der folgende Abschnitt dokumentiert die Dateien in dem `/etc/`-Verzeichnis, welche Benutzer- und Gruppeninformationen unter Red Hat Enterprise Linux speichern.

6.3.2.1. `/etc/passwd`

Die `/etc/passwd`-Datei besitzt eine allgemeine Leseberechtigung und beinhaltet eine Liste von Benutzern, jeweils in einer eigenen Zeile. In jeder Zeile befindet sich eine durch Doppelpunkt abgegrenzte Auflistung mit folgendem Inhalt:

- *Benutzername* — Der Name, den der Benutzer eintippt, um sich im System anzumelden.
- *Passwort* — Beinhaltet das verschlüsselte Passwort (oder ein `x` wenn Schattenpasswörter (Shadow Passwords) benutzt werden— mehr darüber später).
- *Benutzer-ID* (*UID*) — der numerische Gegenwert des Benutzernamens, auf den sich das System und Applikationen beziehen, wenn Zugangsprivilegien festgestellt werden.
- *Gruppen-ID* (*GID*) — der numerische Gegenwert des hauptsächlichen Gruppennamens, auf den sich das System und Applikationen beziehen, wenn Zugangsprivilegien festgestellt werden.
- *GECOS* — Aus historischen Gründen GECOS genannt, ist das GECOS[1]-Feld optional und wird dazu benutzt zusätzliche Informationen zu speichern (wie zum Beispiel den vollen Namen des Benutzers). Mehrere Einträge können hier in einer durch Beistriche unterteilten Liste gespeichert werden. Einrichtungen wie `finger` greifen auf dieses Feld zu, um zusätzliche Benutzerinformation zur Verfügung zu stellen.
- *Heimverzeichnis* — Der absolute Pfad zum Heimverzeichnis des Benutzers, wie z.B. `/home/juan/`.
- *Shell* — Das Programm, das automatisch startet, wann immer sich ein Benutzer anmeldet. Dies ist normalerweise ein Befehls-Interpreter (oft auch eine *shell* genannt). Unter Red Hat Enterprise

1. GECOS steht für 'General Electric Comprehensive Operating Supervisor'. Dieses Feld wurde in der originalen UNIX-Implementation in wissenschaftlichen Laboratorien benutzt. Das Laboratorium hatte viele verschiedene Computer, inklusive einem GECOS. Dieses Feld wurde dazu benutzt, Informationen zu speichern, wenn das UNIX-System Batch-Jobs und Druck-Jobs an das GECOS System sendete.

Linux, ist der standardmäßige Wert `/bin/bash`. Wenn das Feld leer gelassen wird, so wird `/bin/sh` benutzt. Wenn es zu einer nicht-existenten Datei gesetzt ist, kann sich der Benutzer nicht anmelden.

Hier ist ein Beispiel eines `/etc/passwd`-Eintrags:

```
root:x:0:0:root:/root:/bin/bash
```

Diese Zeile zeigt auf, dass der `root`-Benutzer ein Shadow-Passwort besitzt sowie ebenso eine UID und GID lautend auf 0. Der `root`-Benutzer besitzt `/root/` als Heimverzeichnis, und benutzt `/bin/bash` für eine Shell.

Für weitere Informationen über `/etc/passwd`, siehe die`passwd(5)` man-Seite.

6.3.2.2. `/etc/shadow`

Da die `/etc/passwd`-Datei world-readable sein muss (der Hauptgrund dafür liegt in der Benutzung der Datei zur Übersetzung von UID auf den Benutzernamen), ist das Speichern aller Passwörter in `/etc/passwd` mit einem Risiko verbunden. Zugegeben, die Passwörter sind verschlüsselt. Jedoch besteht die Möglichkeit Attacken auf Passwörter zu verüben, sobald das verschlüsselte Passwort vorhanden ist.

Wenn ein Attacker ein Kopie von `/etc/passwd` erlangen kann, so besteht die Möglichkeit, dass insgeheim eine Attacke durchgeführt werden kann. Ohne riskieren zu müssen, bei einem tatsächlichen Anmeldeversuch mit potentiellen, von einem Passwort-Cracker generierten Passwörtern erwischt zu werden, kann ein sog. Attacker einen Passwort-Cracker, wie nachfolgend beschrieben, benutzen:

- Ein Passwort-Cracker generiert potentielle Passwörter
- Jedes potentielle Passwort ist sodann verschlüsselt und benutzt den selben Algorithmus wie das System
- Das verschlüsselte potentielle Passwort wird sodann mit den verschlüsselten Passwörtern in `/etc/passwd` verglichen.

Der gefährlichste Aspekt einer solchen Attacke ist die Tatsache, dass diese auf einem System weit entfernt von Ihrem Unternehmen stattfinden kann. Daher kann der Angreifer die neueste und beste High-Performance-Hardware benutzen, die es ihm ermöglicht eine enorme Anzahl von Passwörtern in kurzer Zeit durchzugehen.

Daher kann die `/etc/shadow`-Datei nur vom Root-Bentuzer gelesen werden und beinhaltet das Passwort (und optionale Passwort-Aging-Information) für jeden einzelnen Benutzer. Wie in der `/etc/passwd`-Datei ist die Information jedes einzelnen Benutzers in einer separaten Zeile. Jede dieser Zeilen ist eine durch Doppelpunkt abgegrenzte Auflistung, welche folgende Infomationen enthält:

- *Benutzername* — Der Name, den der Benutzer eintippt, um sich im System anzumelden. Dies erlaubt der **Login**-Applikation das Passwort des Benutzers abzufragen (und dazugehörige Information).
- *Verschlüsseltes Passwort* — Das 13 bis 24 Zeichen lange Passwort. Das Passwort ist entweder verschlüsselt mittels der `crypt(3)`-Bibliothek-Funktion oder dem md5 Hash-Algorithmus. In diesem Feld werden andere Größen als gültig-formatierte, verschlüsselte oder 'hashed' Passwörter benutzt, um Benutzer-Logins zu kontrollieren und den Passwortstatus aufzuzeigen. Wenn zum Beispiel der Messwert `!` oder `*`anzeigt, ist der Account gesperrt und der Benutzer darf sich nicht anmelden. Wenn der Messwert `!!` anzeigt, so wurde zuvor niemals ein Passwort festgelegt (und der Benutzer, der noch kein Passwort vergeben hat, ist nicht in der Lage sich anzumelden).

- *Datum der letzten Passwort-Änderung* — Die Anzahl der Tage, die vergangen sind, (auch *Epoch* genannt) seitdem das Passwort zuletzt geändert worden ist. Diese Information wird in Zusammenhang mit den Passwort-Aging Feldern benutzt, welche darauf folgen.
- *Anzahl der Tage bevor das Passwort geändert werden kann* — Die Mindestanzahl von Tagen, die vergehen müssen, bevor das Passwort geändert werden kann.
- *Anzahl von Tagen bevor eine Passwort-Änderung erforderlich ist* — Die Anzahl der Tage, welche vergehen müssen, bevor das Passwort wieder geändert werden muss.
- *'Anzahl der Tage'-Warnung vor der Passwort-Änderung* — Die Anzahl der Tage bevor das Passwort abläuft und währenddessen der Benutzer vor dem bevorstehenden Verfall gewarnt wird.
- *Anzahl der Tage bevor der Account deaktiviert wird* — Die Anzahl der Tage nachdem ein Passwort abgelaufen ist und bevor der Account deaktiviert wird.
- *Zeitpunkt seitdem der Account deaktiviert worden ist* — Der Zeitpunkt (gespeichert als Anzahl der Tage seit dem Epoch) seitdem der Benutzer-Account gesperrt worden ist.
- *Ein reserviertes Feld* — Ein Feld das in Red Hat Enterprise Linux ignoriert wird.

Hier ist eine Beispielzeile von `/etc/shadow`:

```
juan:$1$.QKDPc5E$SW1kjRWexrXYgc98F.:12825:0:90:5:30:13096:
```

Diese Zeile zeigt die folgende Information für Benutzer `juan` auf:

- Das Passwort wurde zuletzt am 11. Februar 2005 geändert
- Es gibt keinen erforderlichen Mindestzeitraum bevor das Passwort geändert werden kann
- Das Passwort muss alle 90 Tage geändert werden
- Der Benutzer erhält eine Warnung fünf Tage bevor das Passwort geändert werden muss
- Der Account wird 30 Tage nachdem das Passwort abgelaufen ist und im Falle, dass keine Anmeldeversuche stattgefunden haben, deaktiviert werden
- Der Account wird am 9. November 2005 ablaufen

Für weitere Infomationen zur `/etc/shadow`-Datei, siehe die`shadow(5)` man-Seite.

6.3.2.3. `/etc/group`

Die `/etc/group`-Datei ist world-readable und beinhaltet eine Auflistung von Gruppen, wobei sich jede einzelne in einer eigenen Zeile befindet. Jede Zeile ist eine aus vier durch Doppelpunkte getrennte Felder bestehende Auflistung, welche die folgende Information beinhaltet:

- *Gruppenname* — Der Name der Gruppe. Von verschiedensten Dienstprogrammen als visuell lesbarer Identifikatior für die Gruppe benutzt.
- *Gruppenpasswort* — Wenn gesetzt, ermöglicht es Benutzern, die nicht einer Gruppe angehören, der Gruppe beizutreten, indem der Befehl `newgrp` benutzt wird und das hier gespeicherte Passwort eingetippt wird. Wenn sich ein kleingeschriebenes `x` in diesem Feld befindet, so werden Shadow-Gruppenpasswörter benutzt.
- *Gruppen-ID* (*GID*) — Das numerische Äquivalent zum Gruppennamen. Es wird vom Betriebssystem und Applikationen zur Ermittlung von Zugangsprivilegien benutzt.
- *Mitgliederliste* — Eine durch Beistriche getrennte Auflistung von Benutzern, die zu einer Gruppe gehören.

Hier ist eine Beispielzeile von `/etc/group`:

```
general:x:502:juan,shelley,bob
```

Diese Zeile zeigt auf, dass die `General` Gruppe, die Shadow-Passwörter besitzt, eine Gruppen-ID von 502 besitzt und dass `juan`, `shelley` und `bob` Mitglieder dieser Gruppe sind.

Für weitere Informationen zu `/etc/group`, siehe die`group(5)` man-Seite.

6.3.2.4. `/etc/gshadow`

Die `/etc/gshadow`-Datei kann nur vom Root-Benutzer gelesen werden und beinhaltet ein verschlüsseltes Passwort für jede einzelne Gruppe sowie auch Gruppenmitglieder- und Adminstratorinformationen.Genau wie in der `/etc/group`-Datei, befindet sich die Information jeder einzelnen Gruppe in einer separaten Zeile. Jede einzelne dieser Zeilen ist eine durch Doppelpunkt getrennte Auflistung, welche folgende Informationen enthält:

- *Gruppenname* — Der Name der Gruppe. Von verschiedensten Dienstprogrammen als visuell lesbarer Identifikatior für die Gruppe benutzt.
- *Verschlüsseltes Passwort* — Das verschlüsselte Passwort für die Gruppe. Wenn festgesetzt, ermöglicht es Benutzern, die nicht einer bestimmtenGruppe angehören, der Gruppe beizutreten, indem der Befehl `newgrp` benutzt wird. Wenn der Wert des Feldes `!` ist, ist es keinem Benutzer erlaubt mittels dem `newgrp`-Befehl auf eine Gruppe zuzugreifen. `!!` besitzt den selben Wert wie `!` — zeigt jedoch gleichzeitig an, dass niemals zuvor ein Passwort bestimmt worden ist. Sollte der Wert null sein, so haben nur Gruppenmitglieder Zugang zur Gruppe.
- *Gruppenadministratoren* — Hier aufgelistete Gruppenmitglieder (in einer durch Beistriche getrennten Auflistung) können Gruppenmitglieder hinzufügen oder entfernen mittels dem`gpasswd` -Befehl.
- *Gruppenmitglieder* — Hier aufgelistete Gruppenmitglieder (in einer durch Beistriche getrennten Auflistung) sind reguläre, nicht-administrative Mitglieder der Gruppe.

Hier ist eine Beispielzeile aus `/etc/gshadow`:

```
general:!!:shelley:juan,bob
```

Diese Zeile zeigt, dass `General` Gruppe kein Passwort besitzt und Nicht-Mitgliedern nicht erlaubt beizutreten, indem diese den Befehl `newgrp` verwenden. Zusätzlich dazu ist `shelley` ein Gruppenadministrator und `juan` und `bob` sind reguläre, nicht-administrative Mitglieder.

Da das manuelle Bearbeiten dieser Dateien das Potential für Syntax-Fehler erhöht, wird empfohlen, dass die Applikationen, die mit Red Hat Enterprise Linux für diesen Zweck zur Verfügung gestellt werden stattdessen benutzt werden. Der nächste Abschnitt behandelt die primären Tools, die diese Aufgaben erfüllen.

6.3.3. Benutzer-Account und Gruppen-Applikationen

Dies sind zwei grundsätzliche Arten von Applikationen, welche zum Verwalten von Benutzer-Accounts und Gruppen auf Red Hat Enterprise Linux-System benutzt werden können:

- Die grafische **User Manager**-Applikation
- Eine Folge von Befehlszeilen-Tools

Für detaillierte Instruktionen zur Benutzung des **User Manager**, siehe das Kapitel *Benutzer- und Gruppenkonfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Während die **User Manager**-Applikation und die Befehlszeilen-Dienstprogramme beide hauptsächlich die selbe Aufgabe erfüllen, haben die Befehlszeilen-Tools den Vorteil skript-fähig zu sein und sind deshalb einfacher automatisierbar.

Die folgende Aufstellung beschreibt einige der gebräuchlicheren Befehlszeilen-Tools, die dazu benutzt werden, Benutzer-Accounts und Gruppen zu erzeugen und zu verwalten:

Applikation	Funktion
`/usr/sbin/useradd`	Fügt Benutzer-Accounts hinzu. Dieses Tool wird auch dazu benutzt, primäre und sekundäre Gruppen-Mitgliedschaft zu bestimmen.
`/usr/sbin/userdel`	Löscht Benutzer-Accounts.
`/usr/sbin/usermod`	Bearbeitet Account-Attribute inklusive einiger Funktionen in Zusammenhang mit Passwort-Aging. Für eine noch 'feinkörnigere' Kontrolle, können Sie den Befehl `passwd` benutzen. `usermod` kann auch zum Festlegen von primären und sekundären Gruppenmitgliedschaften benutzt werden.
`passwd`	Setzt Passwörter. Obwohl hauptsächlich zur Änderung von Benutzer-Passwörtern benutzt, werden dadurch gleichzeitig auch alle Aspekte des Passwort-Aging kontrolliert.
`/usr/sbin/chpasswd`	Liest in einer Datei bestehend aus Benutzername und Passwortpaaren und aktualisiert jedes einzelne Benutzerpasswort ordnungsgemäß.
`chage`	Ändert die angewandten Passwort-Aging-Methoden des Benutzers. Der `passwd`-Befehl kann zu diesem Zweck auch benutzt werden.
`chfn`	Ändert die GECOS-Information des Benutzers.
`chsh`	Ändert die standardmäßige Shell des Benutzers.

Tabelle 6-2. Befehlszeilen-Tools zur Benutzter-Verwaltung

Die folgende Auflistung beschreibt einige der gebräuchlicheren Befehlszeilen-Tools, die dazu verwendet werden Gruppen zu erstellen und zu verwalten:

Applikation	Funktion
`/usr/sbin/groupadd`	Fügt Gruppen hinzu, jedoch ohne Zuordnung von Benutzern. Die Programme `useradd` und `usermod` sollten für die Zuordnung von Benutzern zu einer bestehenden Gruppe verwendet werden.
`/usr/sbin/groupdel`	Löscht Gruppen.
`/usr/sbin/groupmod`	Modifiziert Gruppennamen oder GIDs, ändert jedoch nicht die Gruppenmitgliedschaft. Die `useradd` und `usermod`-Programme sollten für die Zuordnung von Benutzern zu einer bestehenden Gruppe verwendet werden.
`gpasswd`	Verändert Gruppenmitgliedschaft und setzt Passwörter, um Nicht-Gruppenmitgliedern, die das Gruppenpasswort kennen, zu ermöglichen, sich der Gruppe anzuschließen. Es wird auch dazu benutzt, Gruppenadministratoren festzulegen.
`/usr/sbin/grpck`	Überprüft die Vollständigkeit von `/etc/group`- und `/etc/gshadow`-Dateien.

Tabelle 6-3. Befehlszeilen-Tools zur Gruppen-Verwaltung

Die soweit aufgelisteten Tools bieten Systemadministratoren große Flexibilität bei der Kontrolle aller Aspekte von Benutzer-Accounts und Gruppen-Mitgliedschaft. Um mehr darüber zu erfahren, siehe die jeweilige man-Seite.

Diese Applikationen legen jedoch nicht fest, welche Ressourcen von diesen Benutzern und Gruppen kontrolliert werden. Dazu muss der Systemadministrator Applikationen zur Vergabe von Dateirechten benutzen.

6.3.3.1. Dateirechte-Applikationen

Dateirechte sind ein wesentlicher Bestandteil in der Verwaltung von Ressourcen innerhalb eines Unternehmens. Die folgende Auflistung beschreibt einige der gebräuchlicheren Befehlszeilen-Tools, die für diesen Zweck verwendet werden.

Applikation	Funktion
`chgrp`	Ändert welche Gruppe eine bestehende Datei besitzt
`chmod`	Ändert Zugangsrechte für eine bestehende Datei. Es ist auch in der Lage spezielle Genehmigungen zuzuordnen.
`chown`	Verändert die Eigentümerschaft einer Datei (und kann ebenso die Gruppe ändern).

Tabelle 6-4. Befehlszeilen-Tools zur Rechteverwaltung

Es ist auch möglich diese Attribute in der grafischen Umgebung von GNOME und KDE zu verändern. Klicken Sie mit der rechten Maustaste auf das Symbol der Datei (zum Beispiel während das Symbol in einem grafischen Dateimanager oder Desktop angezeigt wird) und wählen Sie **Properties**.

6.4. Zusätzliche Ressourcen

Dieser Abschnitt beinhaltet verschiedene Ressourcen, welche dazu benutzt werden können mehr über Account- und Ressource-Management zu lernen und das Red Hat Enterprise Linux-spezifische Thema, welches in diesem Kapitel behandelt wird.

6.4.1. Installierte Dokumentation

Die folgenden Ressourcen werden im Zuge einer typischen Red Hat Enterprise Linux-Installation installiert und können Ihnen dabei helfen, mehr über das in diesem Kapitel behandelte Thema zu lernen.

- **User Manager Help** Menüeintrag — Zur Verwaltung von Benutzer-Accounts und Gruppen.
- `passwd(5)` man-Seite — Lernen Sie mehr über die Dateiformat Information über die `/etc/passwd`-Datei.
- `group(5)` man-Seite — Lernen Sie mehr über die Dateiformat-Information über die `/etc/group`-Datei.
- `shadow(5)` man-Seite — Lernen Sie mehr über die Dateiformat-Information über die `/etc/shadow`-Datei.
- `useradd(8)` man-Seite — Lernen Sie Benutzer-Accounts zu erzeugen oder zu aktualisieren
- `userdel(8)` man-Seite — Lernen Sie, wie man Benutzer-Accounts löscht.

- `usermod(8)` man-Seite — Lernen Sie Benutzer-Accounts zu modifizieren.
- `passwd(1)` man-Seite — Lernen Sie ein Benutzer-Passwort zu aktualisieren.
- `chpasswd(8)` man-Seite — Lernen Sie wie mehrere Benutzer-Passwörter gleichzeitig aktualisiert werden können.
- `chage(1)` man-Seite — Lernen Sie Benutzer-Passwort-Agining-Information zu ändern.
- `chfn(1)` man-Seite — Lernen Sie die GECOS-Information eines Benutzers (`finger`) zu ändern.
- `chsh(1)` man-Seite — Lernen Sie die Login-Shell eines Benutzers zu ändern.
- `groupadd(8)` man-Seite — Lernen Sie eine neue Gruppe zu erzeugen.
- `groupdel(8)` man-Seite — Lernen Sie eine Gruppe zu löschen.
- `groupmod(8)` man-Seite — Lernen Sie eine Gruppe zu modifizieren.
- `gpasswd(1)` man-Seite — Lernen Sie die Dateiein `/etc/group` und `/etc/gshadow` zu verwalten.
- `grpck(1)` man-Seite — Lernen Sie die Vollständigkeit der Dateien `/etc/group` und `/etc/gshadow` zu verifizieren.
- `chgrp(1)` man-Seite — Lernen Sie die Gruppen-Eigentumsberechtigung zu ändern.
- `chmod(1)` man-Seite — Lernen Sie die Datei-Zugangsberechtigungen zu ändern.
- `chown(1)` man-Seite — Lernen Sie die Datei-Eigentumsrechte und Gruppen zu ändern.

6.4.2. Nützliche Webseiten

- http://www.bergen.org/ATC/Course/InfoTech/passwords.html — Ein gutes Beispiel eines Dokumentes, welches Informationen über die Passwort-Sicherheit von Benutzern eines Unternehmens beinhaltet.
- http://www.crypticide.org/users/alecm/ — Die Homepage des Autors eines der populärsten Passwort-Cracking Systeme (Crack). Sie können Crack von dieser Webseite herunterladen und überprüfen wie viele Ihrer Benutzer schwache Passwörter besitzen.
- http://www.linuxpowered.com/html/editorials/file.html — ein guter Überblick über Linux-Dateirechte.

6.4.3. Darauf bezogenen Literatur

Die folgenden Bücher befassen sich mit verschiedensten Themen in Bezug auf Account- und Ressource-Management und sind ebenso nützliche Nachschlagwerke für Red Hat Enterprise Linux-Systemadministratoren.

- The *Red Hat Enterprise Linux Sicherheitshandbuch*; Red Hat, Inc. — Bietet einen Überblick über Sicherheitsaspekte von Benutzer-Accounts, bzw. über die Auswahl von starken Passwörtern.
- The *Red Hat Enterprise Linux Referenzhandbuch*; Red Hat, Inc. — Enthält detaillierte Informationen über die Benutzer und Gruppen, welche in Red Hat Enterprise Linux.vorkommen.
- *Red Hat Enterprise Linux Handbuch zur System-Administration*; Red Hat, Inc. — Beinhaltet ein Kapitel über Benutzer- und Gruppenkonfiguration.
- *Linux Administration Handbook* von Evi Nemeth, Garth Snyder und Trent R. Hein; Prentice Hall — Beinhaltet ein Kapitel über Benutzer-Account-Verwaltung, einen Abschnitt über Sicherheit, der sich auf Benutzer-Account-Dateien bezieht und einen Abschnitt über Datei-Attribute und -Rechte.

Kapitel 7.

Drucker und Drucken

Drucker sind essentiell zur Erstellung einer *Hardcopy* oder Ausdrucks — eine physikalische Abbildung von Daten auf Papier — von Dokumenten zur geschäftlichen, akademischen und privaten Nutzung. Drucker sind zum unabkömmlichen Peripheriegerät in allen Geschäftsebenen und im institutionellen Computergebrauch geworden.

Dieser Abschnitt behandelt die verschiedenen, erhältlichen Drucker und vergleicht deren Nutzung in unterschiedlichen Anwendungsbereichen. Danach wird beschrieben, wie Druckvorgänge von Red Hat Enterprise Linux unterstützt werden.

7.1. Druckertypen

Wie auch bei jedem anderen Computerperipheriegerät gibt es verschiedene Typen von Druckern. Einige Drucker arbeiten mit Technologien, die manuelle, schreibmaschinenartige Funktionalität nachahmen, während andere Drucker Tinte auf Papier sprühen oder mittles Laser ein Image der zu druckenden Seite generieren. Drucker Hardware lässt sich an einen PC oder Netzwerk entweder parallel, seriell oder mittels Daten-Netzwerk-Protokollen anschliessen. Es gibt einige Faktoren, die bei der Beschaffung und dem Einsatz von Druckern in Ihrem EDV-Anwendungsbereich in Betracht gezogen werden müssen.

Die folgenden Abschnitte behandeln die verschiedenen Druckertypen und die Protokolle, die von Druckern dazu benutzt werden, um mit Computern zu kommunizieren.

7.1.1. Erwägungen zum Thema Drucken

Es gibt einige Aspekte die bei der Evaluierung eines Druckers in Betracht gezogen werden müssen. Nachstehend werden einige der üblichsten Kriterien aufgelistet in Bezug auf Ihre Druckbedürfnisse.

7.1.1.1. Funktion

Ihre organisatorischen Bedürfnisse festzulegen und wie ein Drucker diesen Bedürfnissen gerecht werden kann ist ein grundlegendes Kriterium bei der Bestimmung der richtigen Art von Drucker für Ihren Anwendungsbereich. Die wichtigste Frage, die sich hierbei stellt, ist "*Was muss bei uns ausgedruckt werden?*" Da es speziell ausgerichtete Drucker zum Drucken von Text, Bildern oder jeglicher Variation davon gibt, sollten Sie sicher gehen, dass Sie das richtige Werkzeug für Ihre Zwecke beschaffen.

Wenn zum Beispiel der Bedarf nach hoch-qualitativen Farbbildern auf professionellem Kunstdruckpapier besteht, wird empfohlen einen Farbstoffsublimationsdrucker oder einen Farbdrucker mit Thermal-Wachs-Übertragung anstatt eines Laserdruckers oder Anschlagdruckers zu verwenden.

Umgekehrt sind Laser- oder Tintenstrahldrucker bestens geeignet zum Drucken von Rohentwürfen oder Dokumenten, die zum internen Gebrauch bestimmt sind (solche Massen-Drucker werden normalerweise als *Arbeitsgruppen*-Drucker bezeichnet). Die Bedürfnisse des Alltagsbenutzers zu bestimmen, erlaubt Systemadministratoren den richtigen Drucker für die jeweilige Arbeit ausfindig zu machen.

Andere Faktoren, die ebenso in Betracht gezogen werden müssen, sind Features wie *Duplexing* — die Fähigkeit auf beiden Seiten eines Papierblattes zu drucken. Herkömmliche Drucker konnten lediglich auf einer Seite eines Blattes drucken (auch als *Simplex*-Druckvorgang bekannt). Die meisten einfacheren Druckermodelle haben auch heutzutage noch kein standardmäßiges Duplexing. Solche Erweiterungen können einmalige Kosten erheblich in die Höhe treiben. Jedoch auf lange Sicht gesehen kann Duplex-Drucken die Kosten über einen längeren Zeitraum hinweg reduzieren, indem Papier

eingespart wird und dadurch die Kosten im Bereich der *Verbrauchsmaterialien* gesenkt werden können — hauptsächlich Papier.

Ein anderer Faktor, der in Betracht gezogen werden sollte, ist die Papiergröße. Die meisten Drucker können mit den gängigen Papiergrößen umgehen:

- *Letter* — (8 1/2" x 11")
- *A4* — (210mm x 297mm)
- *JIS B5* — (182mm x 257mm)
- *Legal* — (8 1/2" x 14")

Wenn bestimmte Abteilungen (wie zum Beispiel Marketing oder Design) spezielle Bedürfnisse haben, wie die Erstellung von Postern oder Bannern, so gibt es auch sogenannte *Großformat*-Drucker, die auch *A3*-Format (297mm x 420mm) oder kleinformatige Zeitungen (11" x 17") drucken können. Zusätzlich dazu gibt es Drucker, die auch fähig sind sogar noch größere Größen zu drucken, welche aber zumeist nur zu speziellen Zwecken, wie dem Ausdrucken von Plänen benutzt werden.

Zusätzlich dazu sollten High-End-Funktionen, wie zum Beispiel Netzwerkmodule für Arbeitsgruppen- und Drucken von entfernten Einsatzorten in den Evaluierungsprozess miteinbezogen werden.

7.1.1.2. Kosten

Die Kosten sind ein weiterer Faktor, der bei der Drucker-Auswertung in Betracht gezogen werden sollte. Jedoch ist die Festlegung der einmaligen Kosten bei der Anschaffung des Druckers selbst nicht ausreichend. Es gibt andere Kosten, die ebenso in Betracht gezogen werden müssen, wie zum Beispiel Verbrauchsmaterialien, Ersatzteile und Wartung sowie auch Zusätze.

Wie der Name schon sagt, ist Verbrauchsmaterialien ein Allgemeinbegriff, der die Materialien beschreibt, welche während des Druckvorganges aufgebraucht werden. In diesem Falle sind die Verbrauchsmaterialien vorwiegend *Druckmedium* und *Tinte*.

Das Medium ist das Material, auf dem der Text oder das Bild ausgedruckt wird. Die Auswahl des Mediums hängt absolut von der Art von Information ab, die ausgedruckt werden soll.

Wenn Sie zum Beispiel einen Ausdruck eines digitalen Bildes machen möchten, so ist dabei ein spezielles Kunstdruck- oder Hochglanzpapier erforderlich, welches auch für einen längeren Zeitraum natürlicher oder künstlicher Beleuchtung ausgesetzt werden kann und ebenso eine genaue Farbwiedergabe gewährleistet. Diese Vorzüge werden auch als *farbecht* bezeichnet. Für Dokumente, die eine spezielle *Archivierungsgüte* erfordern (wie zum Beispiel Verträge, sonstige rechtliche Papiere und permanente Aufzeichnungen), sollte ein *mattes* (oder Nicht-Glanz-) Papier verwendet werden. Die *Stärke* (oder Dicke) des Papiers spielt ebenfalls eine große Rolle, da manche Drucker eine Papierweiterführung besitzen, die nicht geradlinig, bzw. auf einer Ebene verläuft. Die Benutzung von zu dünnem ode zu dickem Papier kann dabei zu Papierstaus führen. Manche Drucker können ebenfalls auf *transparentem* Papier drucken, was die Abbildung der gedruckten Information mittels Projektor auf einer Leinwand während Präsentationen möglich macht.

Spezial-Medien, wie oben beschrieben können die Kosten der Verbrauchsgüter erheblich beeinflussen und sollten bei der Beurteilung von Druckerbedürfnissen miteinbezogen werden.

Tinte ist ein Allgemeinbegriff, wenn auch nicht alle Drucker flüssige Tinte verwenden. Zum Beispiel benutzern Laserprinter eine Art Pulver, auch als *Toner* bezeichnet, während Anschlagdrucker in Tinte getränkte Farbbänder benutzen. Es gibt auch Spezialdrucker, welche die Tinte während des Druckvorganges aufheizen, während andere Drucker kleinste Tröpfchen Tinte auf das jeweilige Medium sprühen. Die Wiederbeschaffungskosten können daher enorm variieren und hängen auch davon ab, ob der Tintenbehälter *wiederbefüllbar* ist oder ob ein gänzlicher Austausch der *Tintenpatrone* erforderlich ist.

7.2. Anschlagdrucker

Anschlagdrucker verwenden die älteste Drucktechnologie, die sich heute noch in Produktion befindet. Einige der größten Druckerhersteller fahren mit der Erzeugung, dem Vertrieb und dem Support von Anschlagdruckern sowie Teilen und Zubehör fort. Anschlagdrucker sind in speziellen Anwendungsbereichen, in denen kostenfreundliches Drucken erforderlich ist, höchst funktionell. Die drei gängigsten Arten von Anschlagdruckern sind *Punktmatrix-*, *Typenrad-* und *Zeilen*drucker.

7.2.1. Punktmatrixdrucker

Die Technologie, die sich hinter Punktmatrixdruckern verbirgt ist relativ simpel. Das Papier wird gegen eine *Trommel* (ein gummibezogener Zylinder) gepresst und wird mit periodischen Unterbrechungen im Laufe des Druckens vorwärts gezogen. Der elektromagnetisch angetriebene *Druckknopf* bewegt sich über das Papier und schlägt auf das Druckerband, welches sich zwischen dem Papier und der Druckknopfnadel befindet. Der Anschlag der Druckkopfes auf dem Druckerband hinterlässt den Abdruck von Tintenpunkten auf dem Papier, welche lesbare Zeichen formen.

Punktmatrixdrucker unterscheiden sich in Druckauflösung und allgemeiner Qualität durch entweder 9- oder 24-Nadel-Druckköpfen. Je mehr Nadeln pro Zoll, desto besser die Druckqualität. Die meisten Punktmatrixdrucker besitzen eine maximale Auflösung von 240 *dpi* (Punte pro Zoll). Da diese Auflösung nicht so hoch ist, als die von Laser- oder Tintenstrahldruckern, wird bei diesen ein deutlicher Vorteil gegenüber dem Punktmatrixdrucker (oder jeder anderen Art von Anschlagdrucker) sichtbar. Da der Druckkopf die Oberfläche des Papiers mit genügend Kraft anschlagen muss, um Tinte vom Farbband auf das Papier zu transferieren, ist diese Methode ideal für Anwendungsbereiche, die *Durchschläge* erstellen müssen, aufgrund der Benutzung spezieller Durchschreibformulare oder -dokumente. Einzelhändler und Kleinbetriebe benutzen Durchschläge oft als Kassenbons oder Quittungen.

7.2.2. Typenraddrucker

Wenn Sie jemals zuvor mit einer manuellen Schreibmaschine gearbeitet haben, dann verstehen Sie auch das technologische Prinzip von Typenraddruckern. Diese Drucker besitzen Druckköpfe, die aus Metall- oder Plastikrädern bestehen, welche in einzelne *Typenhammer* unterteilt sind. Jeder Typenhammer besitzt die Form eines Buchstabens (als Groß- und Kleinbuchstabe), Nummer oder Satzzeichen. Wenn der Typenhammer gegen das Farbband schlägt, so wird in Form dieses Buchstabens oder Zeichens Tinte auf das Papier gedruckt wird. Typenraddrucker arbeiten geräuschvoll und langsam. Graphiken können nicht gedruckt werden und Schriftarten können ebenfalls nicht gewechselt werden (außer die Druckwelle wird physikalisch ausgetauscht). Typenraddrucker finden heutzutage generell keine Verwendung mehr.

7.2.3. Zeilendrucker

Der *Zeilendrucker* ist eine andere Art von Anschlagdrucker, der irgendwie dem Typenraddrucker ähnlich ist. Jedoch im Gegensatz einem Typendruckrad besitzen Zeilendrucker einen Mechanismus, der es erlaubt mehrere Zeichen gleichzeitig in der selben Zeile zu drucken. Der Mechanismus kann entweder eine große drehende *Drucktrommel* verwenden oder eine schlingenförmige *Druckkette*. Währen die Trommel oder Kette über die Papieroberfläche rotiert, drücken elektromechanische Hämmer, die sich hinter dem Papier befinden, das Papier auf die Oberfläche der Trommel oder Kette, wobei das Papier mit der Form des jeweiligen Zeichens auf der Trommel oder Kette versehen wird.

Aufgrund der Natur des Druckmechanismus sind Zeilendrucker wesentlich schneller als Punktmatrixdrucker oder Typenraddrucker. Jedoch neigen diese dazu, ziemlich laut zu arbeiten und besitzen eine limitierte Fähigkeit in verschiedenen Schriftarten zu drucken und produzieren oft auch eine niedrigere Druckqualität als bei moderneren Drucktechnologien der Fall ist.

Da Zeilenprinter hautpsächlich wegen deren hoher Druckgeschwindigkeit verwendet werden, benutzen diese spezielles *Traktor-zugeführtes* Papier mit einer Lochung entlang jeder Seite. Dies ermöglicht kontinuierliches, unbeaufsichtigtes Hochgeschwindigkeitsdrucken. Ein Anhalten des Druckvorganges ist nur notwendig, wenn eine ganze Schachtel Papier aufgebraucht ist.

7.2.4. Anschlagdrucker Verbrauchsmaterialien

Von allen Druckerarten erzeugen Anschlagdrucker die niedrigsten Kosten in Hinsicht auf Verbrauchsmaterialien. Farbbänder und Papier bilden den Hauptbestandteil laufender Kosten für Anschlagdrucker. Einige Anschlagdrucker (normalerweise Zeilen- oder Punktmatrixdrucker) benötigen Traktor-eingezogenes oder -eingeschobenes Papier, was die Betriebskosten etwas erhöhen kann.

7.3. Tintenstrahldrucker

Ein *Tintenstrahl*drucker benutzt eine der heutzutage populärsten Drucktechnologien. Die relativ günstigen Mehrzweck-Druckmöglichkeiten machen Tintenstrahldrucker zu einer guten Wahl für Klein- und Mittelbetriebe sowie auch für das Heimbüro.

Tintenstrahldrucker benutzen schnelltrocknende, wasserbasierte Tinten und einem Druckkopf mit einer Serie von kleinen Düsen, die Tintetröpfchen auf die Oberfläche des Papiers schleudern. Die Druckkopfanordnung bewegt sich mittels Treibriemen-betriebenem Motor über das Papier.

Tintenstrahler wurden ursprünglich nur zum *monochromen* Drucken (schwarz und weiß) hergestellt. Im Laufe der Zeit wurde der Druckkopf erweitert und die Anzahl der Düsen erhöht, die nun auch die Grundfarben Cyan, Magenta, Yellow und Black beherbergen. Diese Farbkombination (auch *CMYK-Farbmodell* genannt) ermöglicht das Drucken von Bildern mit der nahezu selben Qualität wie ein Fotoentwicklungslabor (wenn eine bestimmte Art von beschichtetem Papier verwendet wird). Alles in allem sind Tintenstrahldrucker eine gute Wahl für S/W und Farbdruckbedarf und liefern generell eine gute bis sehr gute Qualität.

7.3.1. Tintenstrahler Verbrauchsmaterialien

Tintenstrahldrucker sind eher preiswert und liefern wie gesagt eine gute bis sehr gute Druckqualität, besitzen zumeist Zusatzfeatures und die Möglichkeit auch auf größeren Papierformaten zu drucken. Während die Anschaffungskosten eines Tintenstrahldruckers niedriger sind, als die anderer Druckerarten, so dürfen jedoch die allgemeinen Verbrauchskosten nicht außer Acht gelassen werden. Da die Nachfrage an Tintenstrahldruckern groß ist und der Einsatzbereich vom Heimbüro bis zum Großunternehmen reicht, kann die Beschaffung von Verbrauchsmaterialien kostspielig sein.

Anmerkung

Wenn Sie einen Tintenstrahldrucker erwerben möchten, so erkundigen Sie sich nach der Art der benötigten Tintenkartusche(n). Dies ist speziell für Farbeinheiten wichtig. CMYK Tintenstrahldrucker benötigen Tinte für jede der Grundfarben. Wichtig dabei ist jedoch der Umstand, ob jede Farbe in einer eigenen Kartusche aufbewahrt wird oder nicht.

Einige Drucker benutzen lediglich eine Kartusche mit mehreren Kammern. Außer es besteht die Möglichkeit einer Art von Refill-Prozess (Nachfüll-Prozess), muss die gesamte Kartusche ausgetauscht werden, sobald auch nur eine der Farben aufgebraucht ist. Andere Drucker besitzen eine Kartusche mit mehreren Kammern für Farbe, jedoch eine separate Kartusche für Schwarz. In Arbeitsbereichen, wo eine große Menge an Text gedruckt wird, kann diese Art der Anordnung von Vorteil sein. Die beste Lösung ist allerdings einen Drucker mit separaten Kartuschen für jede Farbe

zu finden. Dadurch können Sie dann bequem und einfach lediglich die Farbe austauschen, die aufgebraucht worden ist.

Einige Tintenstrahlhersteller fordern ebenso die Benutzung von speziell behandeltem Papier, um hochqualitative Bilder und Dokumente zu drucken. Diese Art von Papier verwendet mittelmäßige Beschichtungen bis hin zu Hochglanzbeschichtungen, die eigens dazu entwickelt wurden Farbtinten zu absorbieren. Dadurch soll ein sogenanntes *Clumping* (die Tendenz von wasserbasierten Tintenarten in bestimmten Bereichen ineinander zu verlaufen) oder auch ein sogenanntes *banding* (der Ausdruck hat ein gestreiftes Muster bestehend aus störenden Linien) verhindert werden. Berücksichtigen Sie die Druckerdokumentation, wenn es zu empfohlenen Papierarten kommt.

7.4. Laserdrucker

Laserdrucker sind eine andere beliebte Alternative zu Anschlagdruckern. Laserdrucker sind bekannt für deren hohes Ausgabevolumen und der niedrigen Pro-Seite-Kosten. Laserdrucken finden oft in Großbetrieben als Arbeitsgruppen- oder Abteilungsdruckcenter Verwendung, wobei die Leistungsfähigkeit, Dauerhaftigkeit und Druckbedarf eine große Rolle spielen. Da Laserprinter diesen Bedürfnissen in jeder Hinsicht entsprechen (und das bei vernünftigen Pro-Seite-Kosten) ist diese Technologie weitgehend als das Arbeitspferd im Druckbereich von Großunternehmen bekannt.

Laserprinter arbeiten nach einem ähnlichen Prinzip wie ein Fotokopierer. Rollen ziehen ein Blatt Papier aus einem Papierschacht und durch eine *Bildtrommel*, welche statisch geladen ist und dementsprechend das Blatt Papier auflädt. Zur selben Zeit wird eine Drucktrommel entgegengesetzt aufgeladen. Die Oberfläche der Trommel wird sodann mit einem Laser abgetastet. Dort wo der Strahl auftrifft, wird die jeweilige Ladung entfernt. Sind keine Informationen aufzubringen, so bleibt der Laser für den entsprechenden Punkt aus und damit gleichzeitig die Ladung unverändert. Auf die Bildtrommel wird Toner - Pulver aufgebracht, das nur dort haftet, wo der Laser die Ladung gelöscht hat.

Das Papier und die Trommel werden dann miteinander in Kontakt gebracht, wobei der Toner auf das statisch geladene Papier gelangt. Schlussendlich wird der Toner dann durch Erhitzen mittels sogenannten *Fusing Rollers*, auch als Fixierungsrollen/-walzen bezeichnet, auf der Papieroberfläche fixiert.

7.4.1. Farblaserdrucker

Farblaserdrucker sind darauf abgezielt, die besten Merkmale von Laser- und Tintenstrahldruckern in einem Mehrzweckpaket zu vereinen. Die Technologie basiert auf traditionellem, monochromem (Schwarzweiß-) Laserdruck, vereint aber ebenso zusätzliche Komponenten, um Farbbilder und Farbdokumente zu erstellen. Anstatt nur schwarze Tinte zu verwenden, benutzen Farblaserdrucker eine Kombination aus CMYK-Tonern. Die Druckertrommel arbeitet entweder jeweils mit einer einzelnen Farbe und bringt den Toner Farbe um Farbe auf oder auch alle vier Farben gleichzeitig. Die Farben in Form eines vollständigen Bildes werden sodann von der Trommel auf das Papier übertragen. Farblaserprinter setzten ebenso *Fixieröl* nebst den erhitzten Fixierrollen ein, was zur weiteren Fixierung des Farbtoners auf dem Papier führt und verschiedene Glanzstufen beim fertigen Druck erzeugt.

Durch die zusätzlichen Features sind Farbdrucker normalerweise doppelt (oder um ein Vielfaches) so teuer, als reguläre S/W-Laserprinter. In Anbetracht der dadurch erhöhten Gesamtkosten möchten einige Systemadministratoren eventuell monochrome Funktionalität (Text) und Farbfunktionalität (Bild) in Form eines eigens dem monochromen Druck und eines eigens dem Farbdruck gewidmeten Laserdruckers (oder Tintenstrahldruckers) trennen.

7.4.2. Laserdrucker Verbrauchsmaterialien

Abhängig von der Art des eingesetzten Laserdruckers sind die laufenden Kosten für gewöhnlich fix und steigen gleichmäßig mit erhöhter Nutzung oder einer höheren Anzahl an Druckvorgängen. Der Toner wird für gewöhnlich in Kartuschen bereitgestellt, die nach deren Verbrauch einfach ausgetauscht werden. Einige Modelle werden jedoch auch mit nachfüllbaren Kartuschen ausgeliefert. Farblaserprinter benötigen eine Tonerkartusche für jede der vier Grundfarben. Zusätzlich benötigen Farblaserdrucker spezielle Fixierungsöle, um den Toner auf dem Papier zu fixieren sowie Auffangbehälter für Toner-Überschuss. Diese zusätzlichen Betriebsstoffe treiben die Kosten von Verbrauchsmaterialien in die Höhe. Jedoch ist dabei auch zubeachten, dass diese für bis zu 6000 Seiten ausreichen, was durchwegs mehr ist, als die Verbrauchsstoffe-Lebensdauer bei vergleichbaren Tintenstrahl- und Anschlagdruckern. Die richtige Wahl der Papierart ist bei Laserdruckern weitaus weniger wichtig. Dies bedeutet, dass in großen Mengen gekauftes, herkömmliches, xerografisches Papier oder auch Kopierpapier für die meisten Druckvorgänge von ausreichender Qualität ist. Wenn Sie jedoch vorhaben hochqualitative Bilder zu drucken, so sollten Sie jedoch Kunstdruckpapier für ein professionelles Resultat verwenden.

7.5. Andere Druckerarten

Es gibt auch andere Arten von Druckern, die jedoch zumeist speziellen Druckzwecken in professionellen Grafikbüros oder Verlagsgesellschaften dienen. Diese Drucker sind jedoch nicht für den allgemeinen Gebrauch geeignet. Da diese für Nischennutzung bestimmt sind, sind deren Kosten (Anschaffungskosten sowie auch laufende Kosten) auch zumeist höher im Vergleich zu gebrauchsüblichen Druckern.

Thermotransferdrucker

> Diese Drucker werden zumeist für geschäftliche Präsentationsfolien und zum Farb-*Prüfdruck* (Erzeugung von Testdokumenten und Bildern für genaueste Qualitätsprüfung, bevor die Druckvorlage zum Drucken auf industriellen 4-Farb-Offsetdruckern versandt wird) verwendet. Thermotransferdrucker benutzen eine Folie, auf der sich wachsartige Farben befinden. Eine Zeile aus Thermoelementen erhitzt die Folie punktweise und schmilzt dabei die Farbe mit etwa hundert Grad Celsius auf das Papier.

Farbstoffsublimationsdrucker

> Wird in Unternehmen wie zum Beispiel Dienstleistungsunternehmen verwendet — wo professionelle Qualitätsdokumente, Folder und Präsentationen wichtiger sind als Verbrauchsmaterialkosten — Farbsublimationsdrucker sind die Arbeitspferde im Bereich qualitativen CMYK-Druckens. Das Konzept hinter den Farbsublimationsdruckern ist ähnlich dem von Thermotransferdruckern mit dem einzigen Unterschied, dass eine sich verbreitende Plastikfarbenschicht anstatt des farbigen Wachses verwendet wird. Der Druckkopf heizt die farbige Schicht auf und vaporisiert das Bild auf ein speziell beschichtetes Papier.
>
> Farbsublimation ist sehr beliebt in der Design- und Verlagswelt sowie auch im Bereich wissenschaftlicher Forschung, wo Präzision und Detailgenauigkeit eine grosse Rolle spielen. Solche Druckqualität und Präzision hat ihren Preis. Farbsublimationsdrucker sind bekannt für deren hohe Kosten pro Seite.

Volltontintendrucker

> Zumeist in der Verpackungsindustrie und Industriedesignbereich anzutreffen, sind Volltontintendrucker dazu ausgerichtet, auf einer Vielzahl von verschiedenen Papierarten drucken zu können. Volltontintendrucker benutzen gehärtete Tintenstäbe, die geschmolzen werden und durch schmale Düsen auf dem Druckkopf versprüht werden. Das Papier wird danach durch eine Fixierrolle geschickt, welche die Tinte auf der Papieroberfläche fixiert.

Der Volltontintendrucker ist ideal zum Erstellen von Prototypen bzw. zum Erstellen von Prüfdrucken von neuen Designs für Produktverpackungen. Daher besteht bei den meisten Serviceorientierten Betrieben kein Bedarf für eine solche Art von Drucker.

7.6. Druckersprachen und Technologien

Vor der Einführung der Laser- und Tintenstrahltechnologie konnten Anschlagdrucker lediglich Standardtext ohne Variationen in Schriftgröße und Schriftart ausdrucken. Heutzutage sind Drucker in der Lage, komplexe Dokumente mit eingebauten Bildern, Schaubildern und tabellarischen Darstellungen in mehreren Rahmen und in verschiedenen Sprachen auf ein und derselben Seite darzustellen. Solche Komplexität muss einige Formatkonventionen befolgen. Dies führte zur Entwicklung der *Page Description Language* (Seitenbeschreibungssprache oder PDL) — eine spezielle Dokumentenformatierungssprache, die zur Kommunikation der Druckers mit dem Computer entwickelt worden war.

Im Laufe der Jahre haben Druckerhersteller deren eigene, proprietäre Sprachen entwickelt, um Dokumentenformate zu beschreiben. Jedoch bezogen sich diese Sprachen lediglich auf die hauseigenen Drucker. Wenn Sie zum Beispiel eine druckfertige Datei mittels proprietärer PDL zu einer professionellen Presse gesandt hätten, so hätte es keinerlei Garantie gegeben, dass Ihre Datei kompatibel mit den Druckmaschinen gewesen wäre.

Xerox® entwickelte das Interpress™-Protokoll für deren Druckerpalette, jedoch konnte die Adoption dieses Protokolls durch den Rest der Druckerindustrie nie realisiert werden. Zwei der ursprünglichen Entwickler von Interpress verliessen Xerox und gründeten Adobe®, eine Softwarefirma, welche ausschließlich grafisch orientierte Betriebe auf dem elektronischen Sektor und auf Dokumente spezialisierte Firmen versorgte. Adobe entwickelte ein weitgehend eingesetztes PDL, *PostScript*™ genannt, welches eine Markup-Language oder Auszeichnungssprache verwendet, um Textformatierung und Image-Informationen wiederzugeben, welche von Druckern verarbeitet werden kann. Zur selben Zeit entwickelte Hewlett-Packard® die *Printer Control Language*™ (oder PCL) zur Benutzung in deren allgegenwärtigen Laser- und Tintenstrahldrucker-Artikeln. PostScript und PCL sind nun weitgehend verwendete PDLs und werden von den meisten Druckerherstellern unterstützt.

PDLs arbeiten auf dem selben Prinzip wie Programmiersprachen. Wenn ein Computer zum Drucken bereit ist, so nimmt der PC oder der Arbeitsplatzrechner die Bilder, typografischen Informationen und Dokumentenlayouts und benutzt diese als Objekte, die Instruktionen für den Drucker zur Weiterverarbeitung darstellen. Der Drucker übersetzt diese Objekte sodann in *Raster*, einer Serie von gescannten Linien, die ein bildliche Darstellung des Dokuments erzeugen (auch *Rasterbildverarbeitung (Raster Image Processing)* oder RIP genannt) und druckt diese Ausgabe als ein Bild auf eine Seite; komplett mit Text und Grafiken. Dieser Arbeitsablauf macht das Drucken von Dokumenten jeglicher Komplexität einheitlich und definiert einen Standard, der zu sehr geringen oder gar keinen Variationen beim Drucken auf verschiedenen Druckern führt. PDLs sind auf jedes Format übertragbar und ebenso auf jede Papiergröße.

Die Auswahl des richtigen Druckers hängt vom Standard ab, den die verschiedenen Abteilungen in Ihrem Unternehmen gesetzt haben, um deren Bedürfnisse abzudecken. Die meisten Abteilungen benutzen Textverarbeitungs- und andere Produktivitätssoftware, welche PostScript-Sprache zur Ausgabe an Drucker verwenden. Wenn Ihre Grafikabteilung jedoch PCL verwendet oder eine andere proprietäre Form des Drucks verwendet, so sollten Sie diesem Umstand ebenso Beachtung schenken.

7.7. Vernetzte versus lokale Drucker

Abhängig von den Bedürfnissen Ihrer Organisation ist es wahrscheinlich unnotwendig, jedem Mitglied einen eigenen Drucker zur Verfügung zu stellen. Dies könnte festgelegte Budgets schmälern, was gleichzeitig auch das Vorhandensein von geringerem Kapital für andere wichtige Anschaffungen bedeuten würde. Während lokale Drucker, die parallel oder mittels USB-Verbindung mit jedem lokalen Arbeitsplatz verbunden sind, eine ideale Lösung für den Benutzer selbst darstellen würden, so ist dies normalerweise ökonomisch nicht zulässig.

Druckerhersteller haben darauf mit der Entwicklung von *Abteilungsdruckern* (oder Arbeitsgruppendruckern) reagiert. Diese Geräte sind normalerweise langlebig, schnell und besitzen Verbrauchsmaterialien mit relativ langer Lebensdauer. Arbeitsgruppen-Drucker sind normalerweise mit einem Druckserver verbunden, einem Einzelgerät (wie zum Beispiel einen rekonfigurierten Arbeitsplatzrechner), das Druckaufträge bearbeitet und die Ausgabe zum jeweils ausgewählten Drucker weiterleitet. Neuere Versionen von Abteilungs-Druckern besitzen bereits eingebaute (oder als Erweiterung bestehende) Netzwerk-Schnittstellen, wodurch kein Bedarf mehr nach einem eigenen Druckserver besteht.

7.8. Red Hat Enterprise Linux-spezifische Information

Der folgende Abschnitt beschreibt die verschiedenen Merkmale von Red Hat Enterprise Linux, die sich auf Drucker beziehen.

Mit der Anwendung **Printer Configuration Tool** können Benutzer einen Drucker konfigurieren. Mit diesem Tool können Sie die Drucker-Konfigurationsdatei, DruckerSpool-Verzeichnisse und Druckfilter warten.

Red Hat Enterprise Linux 4 verwendet das CUPS Drucksystem. Wenn ein System von einer vorherigen Version von Red Hat Enterprise Linux das CUPS verwendet, aktualisiert wurde, erhält die Aktualisierung die Konfiguration der Warteschlangen.

Um das **Printer Configuration Tool** verwenden zu können, müssen Sie über root-Berechtigungen verfügen. Wählen Sie zum Starten der Anwendung **Hauptmenü** (auf dem Panel) **=> Systemeinstellungen => Printing** oder geben Sie den Befehl `system-config-printer` ein. Dieser Befehl legt automatisch fest, ob die Grafikversion oder die text-basierte Version gestartet werden soll, abhängig davon, ob der Befehl in der grafischen X Window Systemumgebung oder von einer text-basierten Konsole aus eingegeben wird.

Sie können das **Printer Configuration Tool** auch zur Ausführung als text-basierte Version zwingen, indem Sie den Befehl `system-config-printer-tui` von einem Shell-Prompt aus ausführen.

Wichtig

Ändern Sie nicht die Datei `/etc/printcap` oder die Dateien im `/etc/cups/` Verzeichnis. Jedes Mal, wenn der Drucker-Daemon (`cups`) gestartet oder neu gestartet wird, werden neue Konfigurationsdateien dynamisch erstellt. Diese Dateien werden auch dynamisch erstellt, wenn Änderungen über das **Printer Configuration Tool** durchgeführt werden.

Abbildung 7-1. Printer Configuration Tool

Die folgenden Druckerwarteschlangen-Typen können konfiguriert werden:

- **Lokal-verbunden** — ein Drucker, der direkt durch einen parallelen oder USB-Port an den Computer angeschlossen ist.
- **CUPS im Netzwerk (IPP)** — ein Drucker, der an ein anderes CUPS-System angeschlossen ist, auf den über ein TCP/IP Netzwerk zugegriffen werden kann (zum Beispiel ein Drucker, der an ein anderes Red Hat Enterprise Linux System angeschlossen ist, und bei dem CUPS übers Netzwerk läuft).
- **UNIX im Netzwerk (LPD)** — ein Drucker, der an ein anderes UNIX-System angeschlossen ist, auf den über ein TCP/IP Netzwerk zugegriffen werden kann (zum Beispiel ein Drucker, der an ein anderes Red Hat Enterprise Linux System angeschlossen ist, und bei dem LPD übers Netzwerk läuft).
- **Windows im Netzwerk(SMB)** — Ein Drucker, der an ein anderes System angeschlossen ist, das einen Drucker über ein SMB Netzwerk gemeinsam verwendet (zum Beispiel ein Drucker, der an einen Microsoft Windows™ Computer angeschlossen ist).
- **Novell im Netzwerk(NCP)** — Ein Drucker, der an ein anderes System angeschlossen ist, das die Netzwerktechnologie von Novell Netware verwendet.
- **JetDirect im Netzwerk** — ein Drucker, der direkt über HP JetDirect anstelle eines Computers an das Netzwerk angeschlossen ist.

Wichtig

Wenn Sie eine neue Druckwarteschlange hinzufügen oder eine vorhandene Warteschlange modifizieren, müssen Sie die Änderungen übernehmen, damit diese wirksam werden.

Wenn Sie auf den Button **Anwenden** klicken, werden alle Änderungen gespeichert und der Drucker-Daemon neu gestartet. Die Änderungen werden nicht in die Konfigurationsdatei geschrieben, bis der Drucker-Daemon neu gestartet wird. Alternativ hierzu können Sie erst auf **Datei => Änderungen speichern** und dann **Aktion => Übernehmen** klicken.

Für nähere Informationen zur Druckerkonfiguration unter Red Hat Enterprise Linux siehe *Red Hat Enterprise Linux Handbuch zur System-Administration*.

7.9. Zusätzlich Quellen

Druckerkonfiguration und Drucken im Netzwerk sind weitläufige Themen, die einen bestimmten Wissensgrad und Erfahrung im Bereich Hardware, Vernetzung und Systemadministration erfordern. Für nähere Informationen zum Einsatz von Druckerdiensten in Ihren Arbeitsbereichen, beziehen Sie sich bitte auf folgende Quellen:

7.9.1. Installierte Dokumentation

- `lpr(1)` man-Seite — Lernen Sie bestimmte Dateien auf dem Drucker Ihrer Wahl auszudrucken.
- `lprm(1)` man-Seite — Lernen Sie mehr über das Entfernen einer Druckanfrage von einer Drucker-Warteschlange.
- `cupsd(8)` man-Seite — Lernen Sie mehr über den CUPS (Common Unix Printer System) Drucker-Daemon.

- `cupsd.conf(5)` man-Seite — Lernen Sie über das Dateiformat für die CUPS Drucker-Daemon-Konfigurationsdatei.
- `classes.conf(5)` man-Seite — Lernen Sie über das Dateiformat für die CUPS Klassen-Konfigurationsdatei.
- Dateien in `/usr/share/doc/cups-<version>` — Lernen Sie mehr über das CUPS Druck-System.

7.9.2. Nützliche Websites

- http://www.webopedia.com/TERM/p/printer.html — Allgemeine Definitionen von Druckern und Beschreibungen von Druckerarten.
- http://www.linuxprinting.org/ — Eine Datenbank bestehend aus Dokumenten über Drucken, gemeinsam mit einer Datenbank von nahezu 1000 Druckern, die mit Linux-Druckeinrichtungen kompatibel sind.
- http://www.cups.org/ — Dokumentation, FAQs und News-Gruppen zum Thema CUPS.

7.9.3. Themenbezogene Literatur

- *Network Printing* von Matthew Gast und Todd Radermacher; O'Reilly & Associates, Inc. — Umfassende Information über die Benutzung von Linux als Druck-Server in heterogenen Umgebungen.
- *Red Hat Enterprise Linux Handbuch zur System-Administration*; Red Hat, Inc. — Beinhaltet ein Kapitel über Druckerkonfiguration.

Kapitel 8.

Auf das Schlimmste vorbereiten

Das Vorbereiten auf Katastrophen ist ein Thema, das leicht von Systemadministratoren vernachlässigt wird — es ist unangenehm und irgendwie kommt doch immer etwas Dringenderes dazwischen. Katastrophenvorbereitung zu vernachlässigen ist jedoch das Schlimmste, was ein Systemadministrator tun kann.

Auch wenn einem die eher dramatischen Katastrophen (wie Feuer, Überflutung oder Sturm) zuallererst in den Sinn kommen, können die geringeren Probleme wie versehentlich durchtrennte Stromleitungen oder ein Rohrbruch genauso starke Auswirkungen haben. Daher ist die Definition einer Katastrophe, die ein Systemadministrator im Hinterkopf behalten sollte, eher die eines ungeplanten Ereignisses, das den Arbeitsfluss in einem Unternehmen unterbricht.

Während es unmöglich ist, alle verschiedenen Katastrophentypen aufzulisten, untersucht dieser Abschnitt die Hauptfaktoren, die Teil einer jeden Katastrophe sind. Mögliche Risiken können somit nicht aufgrund ihrer Wahrscheinlichkeit, sondern aufgrund der Faktoren, die zur Katastrophe führen können, untersucht werden.

8.1. Arten von Katastrophen

Im allgemeinen gibt es vier verschiedene Faktoren, die eine Katastrophe auslösen können. Diese sind:

- Hardware-Ausfälle
- Software-Ausfälle
- Umgebungs-Ausfälle
- Menschliches Versagen

8.1.1. Hardware-Ausfälle

Hardware-Ausfälle sind leicht zu verstehen — die Hardware fällt aus und die Arbeit kommt zum Stillstand. Was schwieriger zu verstehen ist, sind die Gründe für einen Ausfall und inwieweit die Risiken reduziert werden können. Hier sind einige Vorschläge:

8.1.1.1. Ersatz-Hardware bereithalten

Im einfachsten Fall kann das Risiko durch Hardware-Ausfälle durch das Bereithalten von Ersatz-Hardware reduziert werden. Diese Maßnahme erfordert jedoch zwei Voraussetzungen:

- Es gibt jemanden vor-Ort, der das Problem diagnostizieren, die ausgefallene Hardware identifizieren und diese austauschen kann.
- Ersatz für die ausgefallene Hardware steht zur Verfügung.

Diese Themen werden später in größerem Detail behandelt.

8.1.1.1.1. Fähigkeiten

Abhängig von Ihrer Erfahrung und der betroffenen Hardware steht die Kompetenz eventuell gar nicht zur Debatte. Wenn Sie jedoch vorher noch nicht mit Hardware gearbeitet haben, sollten Sie sich vielleicht bei einem Anfängerkurs zur PC-Reparatur an der Volkshochschule in Ihrem Ort anmelden.

Auch wenn solche Kurse Sie nicht unbedingt auf das Lösen von Problemen von großen Servern vorbereiten oder gar darauf ausgelegt sind, bieten sie jedoch eine gute Methode, mit den Grundlagen (richtiger Umgang mit Werkzeugen und Komponenten, grundlegende Diagnose etc.) vertraut zu werden.

Tipp

Bevor Sie den Versuch unternehmen, das Problem selbst zu lösen, sollten Sie sicherstellen, dass die betroffene Hardware:

- Keiner Garantie mehr unterliegt
- Keinem Service/Wartungsvertrag jeglicher Art unterliegt

Wenn Sie versuchen, Hardware zu reparieren, die noch durch eine Garantie und/oder Servicevertrag abgedeckt ist, verletzen Sie höchstwahrscheinlich die Vertragsbedingungen und setzen eine weiterführende Abdeckung aufs Spiel.

Es ist jedoch auch mit den geringsten Kenntnissen möglich, ausgefallene Hardware zu diagnostizieren und zu ersetzen — vorausgesetzt, Sie wählen Ihren Bestand an Ersatz-Hardware mit Bedacht.

8.1.1.1.2. Ersatzteilbestand

Die Frage nach dem richtigen Bestand beschreibt die vielschichtige Natur der Wiederherstellung. Wenn Sie überlegen, von welcher Hardware einen Bestand anzulegen, sollten Sie folgende Dinge im Hinterkopf behalten:

- Maximale Ausfallzeit
- Die Fähigkeiten, die zur Reparatur benötigt werden
- Budget für Ersatzteile
- Lagerplatz für Ersatzteile
- Andere Hardware, für welche die gleichen Ersatzteile verwenden werden können

Jeder dieser Punkte hat Auswirkungen auf die Art der Ersatzteile, die gelagert werden sollen. So reduziert zum Beispiel das Lagern gesamter Systeme die Ausfallzeit erheblich und erfordert nur geringe Fähigkeiten für die Installation. Diese Vorgehensweise ist jedoch auch wesentlich teurer als ein Ersatz-CPU und RAM-Modul im Schrank. Die Kosten können sich jedoch lohnen, wenn Ihr Unternehmen mehrere Dutzend identische Server besitzt, die von einem einzigen Ersatzsystem profitieren können.

Unabhängig von der letztendlichen Entscheidung ist die nächste Frage unvermeidlich und wird als nächstes behandelt.

8.1.1.1.2.1. Wieviele Ersatzteile lagern?

Die Frage nach den Ersatzteilbeständen ist auch vielschichtig. Hier sind die Hauptpunkte:

- Maximale Ausfallzeit
- Voraussichtliche Ausfallrate
- Geschätzte Zeit der Wiederbeschaffung
- Budget für Ersatzteile

- Lagerplatz für Ersatzteile
- Andere Hardware, für welche die gleichen Ersatzteile verwenden werden können

Für Systeme, die eine Ausfallzeit von 2 Tagen verkraften können und für ein Ersatzteil, das einmal im Jahr verwendet wird und innerhalb eines Tages wiederbeschafft werden kann, ist es sinnvoll, nur ein Ersatzteil zu haben (oder gar keines, wenn Sie sich sicher sind, ein Ersatzteil innerhalb von 24 Stunden beschaffen zu können).

Für Systeme, die maximal nur einige Minuten ausfallen dürfen und für ein Ersatzteil, das einmal im Monat verwendet wird (und mehrere Wochen in der Wiederbeschaffung braucht) ist es sinnvoll, dass ein halbes Dutzend (oder mehr) Ersatzteile gelagert werden.

8.1.1.1.3. Ersatzteile, die gar keine sind

Wann ist ein Ersatzteil gar kein Ersatzteil? Wenn es allgemein im täglichen Job verwendet wird, jedoch einem hochrangigeren System als Ersatzteil dient, falls dies notwendig wird. Dieser Ansatz hat einige Vorteile:

- Weniger finanzielle Ressourcen für "unproduktive" Ersatzteile aufwenden
- Die Hardware ist funktionstüchtig

Es gibt jedoch auch einige Nachteile bei dieser Methode:

- Die normale Produktion der niederrangigen Aufgabe wird unterbrochen
- Es entsteht ein Risiko, sollte die niederrangige Hardware ausfallen (und damit kein Ersatzteil für die höherrangige Hardware lassen)

Vor dem Hintergrund dieser Einschränkungen kann das Verwenden eines anderen Produktions-Systems als Ersatz funktionieren. Der Erfolg hängt jedoch von der systemspezifischen Last und den Auswirkungen ab, die der Ausfall des Systems auf die Vorgänge im Datenzentrum hat.

8.1.1.2. Serviceverträge

Serviceverträge lassen Hardware-Ausfälle zum Problem anderer werden. Alles, was Sie tun müssen, ist zu bestätigen, dass tatsächlich ein Ausfall aufgetreten ist und dies nicht durch einen Softwarefehler hervorgerufen worden ist. Dann tätigen Sie einen Telefonanruf und jemand kommt vorbei, der die Probleme behebt.

Es scheint so einfach. Wie jedoch mit den meisten Dingen im Leben, steckt mehr dahinter als es den Anschein hat. Hier einige Dinge, die Sie berücksichtigen sollten, wenn Sie einen Servicevertrag abschließen wollen:

- Verfügungsstunden
- Reaktionszeit
- Verfügbarkeit von Ersatzteilen
- Verfügbares Budget
- Zu ersetzende Hardware

In den folgenden Abschnitten wird jedes Einzelne dieser Details näher besprochen.

8.1.1.2.1. Verfügungsstunden

Es sind je nach Bedürfnis verschiedene Serviceverträge erhältlich. Eine der großen Variablen zwischen den verschiedenen Verträgen sind die Verfügungsstunden. Wenn Sie nicht in der Lage sind, eine gewisse Summe für das Privileg zu bezahlen, können Sie nicht jederzeit anrufen und erwarten, dass ein Techniker kurze Zeit später vor der Tür steht.

Abhängig von Ihrem Vertrag kann es sein, dass Sie die Wartungsfirma nur an einem bestimmten Tag/zu einer bestimmten Zeit anrufen können oder auch die Firma eventuell erst nach einer bestimmten Zeit/an einem bestimmten Tag einenTechniker vorbeischickt.

Die meisten Verfügungsstunden werden in Stunden und Tagen festgelegt, an denen ein Techniker Ihnen im Problemfall zur Verfügung steht. Einige der häufigeren Verfügungsstunden sind:

- Montag bis Freitag, 09:00 bis 17:00 Uhr.
- Montag bis Freitag, 12/18/24 Stunden pro Tag (mit gemeinsam vereinbarten Beginn- und Endzeiten)
- Montag bis Samstag (oder Montag bis Sonntag), Zeiten wie oben

Wie Sie wahrscheinlich erwarten, erhöhen sich die Vertragskosten mit den Verfügungsstunden. Im allgemeinen kostet das Erweitern der Deckung Montag bis Freitag weniger als das Hinzufügen von Samstags- und Sonntagsdeckung.

Aber auch hier können Sie die Kosten reduzieren, wenn Sie einige Arbeiten selbst durchführen.

8.1.1.2.1.1. Depot-Service

Erfordert Ihre Situation nichts weiter als einen Techniker während allgemeiner Geschäftszeiten und verfügen Sie über ausreichend Erfahrung, so dass Sie feststellen können, was repariert werden muss, sollten Sie sich den *Depot-Service* ansehen. Unter vielen Namen, wie *Walk-In Service* oder *Drop-Off Service* bekannt, haben einige Hersteller Service-Depots, in denen Techniker die vom Kunden vorbeigebrachte Hardware reparieren.

Der Depot-Service hat den Vorteil, dass er genauso schnell ist wie Sie. Sie müssen nicht auf technisches Personal warten. Mitarbeiter in einem Depot kommen nicht zum Kunden, was bedeutet, dass sofort jemand Ihre Hardware reparieren kann, sobald Sie diese zum Depot gebracht haben.

Da der Depot-Service zentral durchgeführt wird, stehen die Chancen auf verfügbare Ersatzteile ziemlich gut. Dies kann Ersatzteillieferungen über Nacht oder das Warten auf Ersatzteile, die erst hunderte von Kilometern von einer anderen Geschäftsstelle geliefert werden müssen, verhindern.

Es gibt jedoch auch einige Nachteile. Der Offensichtlichste ist, dass Sie sich die Servicestunden nicht aussuchen können — Sie erhalten Service, wenn das Depot offen ist. Ein weiterer Aspekt ist, dass die Techniker zu einer bestimmten Zeit Feierabend machen. Fällt Ihr System also am Freitag um 16:30 Uhr aus und Sie erreichen das Depot um 17:00 Uhr, bleibt die Reparatur bis Montag morgen liegen.

Ein weiterer Nachteil ist, dass der Depot-Service von einem nahegelegenen Depot abhängt. Befindet sich Ihr Unternehmen im Stadtbereich, ist dies wahrscheinlich kein großes Problem. Sind Sie jedoch eher auf dem Land oder außerhalb der Stadt angesiedelt, kann das nächste Depot ziemlich weit weg sein.

Tipp

Wenn Sie sich für den Depot-Service entscheiden, denken Sie bitte einen Moment darüber nach, wie die Hardware zum Depot geliefert werden soll. Haben Sie einen Firmenwagen oder Ihr eigenes Auto? Falls Sie Ihren eigenen Wagen verwenden, haben Sie genügend Platz und Kapazitäten? Wie sieht es mit der Versicherung aus? Werden mehr als eine Person für das Auf- und Entladen der Hardware benötigt?

Auch wenn diese Fragen relativ einfach erscheinen, sollten diese angesprochen werden, bevor die Entscheidung für einen Depot-Service gefällt wird.

8.1.1.2.2. Reaktionszeit

Zusätzlich zu den Verfügungsstunden geben viele Servicevereinbarungen eine bestimmte Reaktionszeit vor. Mit anderen Worten: Wie lange dauert es, bis Sie nach Ihrer Serviceanfrage einen Techniker zur Verfügung haben? Wie Sie sich denken können, resultiert eine schnellere Reaktionszeit in einem teureren Vertrag.

Die zur Verfügung stehenden Reaktionszeiten unterliegen gewissen Einschränkungen. So hat zum Beispiel die Anfahrtszeit vom Hersteller zu Ihrem Unternehmen einen großen Einfluss auf die möglichen Reaktionszeiten[1]. Reaktionszeiten um die vier Stunden werden allgemein als schnell betrachtet. Langsamere Reaktionszeiten reichen von acht Stunden (was effektiv gesehen zum Service am "nächsten Tag" innerhalb einer Standard-Geschäftsvereinbarung wird), bis zu 24 Stunden. Wie bei jeden anderen Aspekt der Vereinbarung sind diese Zeiten verhandelbar — für die richtige Summe.

Anmerkung

Auch wenn es nicht häufig vorkommt, sollten Sie sich doch bewusst sein, dass einige Servicevereinbarungen mit Reaktionszeitregelungen den Service eines Herstellers vollkommen auslasten können. Es ist nicht ganz unbekannt, dass vollkommen ausgelastete Unternehmen jemanden — *irgendjemanden* — zu einem Serviceanruf mit kurzer Reaktionszeit schicken, nur um die Reaktionsklausel einzuhalten. Diese Person diagnostiziert dann angeblich das Problem, und ruft dann das "Hauptquartier" an, damit jemand "das richtige Ersatzteil" bringt.

Tatsächlich wird jedoch nur auf die Person gewartet, die dann wirklich in der Lage ist, das Problem zu beheben.

Während dies unter besonderen Umständen verständlich ist (wenn zum Beispiel ein Stromausfall Systeme im gesamten Servicebereich lahmgelegt haben), sollten Sie, falls dies Verhalten öfter auftritt, den Servicemanager benachrichtigen und eine Erklärung verlangen.

Sind Ihre Ansprüche an die Reaktionszeit sehr hoch (und Sie verfügen über das entsprechend hohe Budget), gibt es einen Ansatz, bei dem Sie die Reaktionszeiten noch weiter senken können — auf Null.

8.1.1.2.2.1. Gar keine Reaktionszeit — ein Techniker vor-Ort

In angemessener Situation (Sie sind einer der größten Kunden in der Gegend), ausreichend Bedarf (*jegliche* Downtime ist inakzeptabel) und ausreichenden finanziellen Ressourcen (wenn Sie nach dem Preis fragen müssen, können Sie sich es wahrscheinlich nicht leisten), sind Sie eventuell ein Kandidat für einen Vollzeit-Techniker vor-Ort. Die Vorteile eines ständig verfügbaren Technikers sind offensichtlich:

- Sofortige Reaktion auf jegliche Probleme

1. Und dies wäre die bestmögliche Reaktionszeit, da technisches Personal meistens für eine ganze Gegend verantwortlich ist, die sich in alle Richtungen um das Hauptquartier erstrecken kann. Wenn Sie sich an einem Ende des Bereichs befinden und der einzig verfügbare Techniker am anderen Ende ist, dann ist die Reaktionszeit wesentlich länger

- Eine proaktive Herangehensweise an die Systemwartung

Wie Sie sich denken können, kann diese Option *sehr* kostspielig werden, insbesondere, wenn Sie einen Techniker 24/7 benötigen. Wenn dies jedoch für Ihr Unternehmen angemessen ist, sollten Sie eine Reihe von Punkten im Hinterkopf behalten, um den größten Nutzen hieraus zu ziehen.

Als erstes benötigen Techniker vor-Ort viele der Ressourcen eines normalen Mitarbeiters wie zum Beispiel einen Arbeitsplatz, Telefon, Zugangskarten und/oder Schlüssel und so weiter.

Vor-Ort Techniker sind nur dann wirklich von Vorteil, wenn die richtigen Ersatzteile zur Verfügung stehen. Stellen Sie daher eine sichere Lagerstätte für Ersatzteile zur Verfügung. Zusätzlich dazu sollte der Techniker einen angemessenen Lagerbestand der Ersatzteile für Ihre Konfiguration führen und sicherstellen, dass diese Teile nicht regelmäßig von anderen Technikern für eigene Zwecke "ausgeschlachtet" werden.

8.1.1.2.3. Teile-Verfügbarkeit

Offensichtlich spielt die Verfügbarkeit von Ersatzteilen eine große Rolle bei der Eingrenzung des Risikos für Hardware-Ausfälle. Im Kontext einer Servicevereinbarung nimmt die Verfügbarkeit der Ersatzteile eine andere Dimension ein, da diese nicht nur auf Ihr Unternehmen zutrifft, sondern auf alle Kunden im Einzugsbereich des Herstellers, die diese Teile eventuell auch benötigen. Ein anderes Unternehmen, das vielleicht eine größere Menge Hardware von dem betreffenden Hersteller abgenommen hat als Ihr Unternehmen wird u.U. auch bevorzugt behandelt, wenn es um Ersatzteile (oder Techniker) geht.

Leider kann in diesem Fall nicht getan werden, abgesehen von einem Gespräch mit dem Service-Manager.

8.1.1.2.4. Budget

Wie bereits erwähnt variieren Servicevereinbarungen im Preis, je nach Art von bereitgestelltem Service. Denken Sie daran, dass die Kosten für einen Wartungsvertrag ein periodisch wiederkehrender Aufwand ist; jedes Mal, wenn der Vertrag ausläuft, müssen Sie einen neuen Vertrag aushandeln und neuerdings die Summe bezahlen.

8.1.1.2.5. Abzudeckende Hardware

Hier ist ein Bereich, für den Sie die Kosten so gering als möglich halten können. Stellen Sie sich vor, Sie haben eine Servicevereinbarung mit einem ’24 Stunden rund um die Uhr’-Techniker vor-Ort , Ersatzteile vor-Ort — alles was das Herz begehrt. Jedes Stück Hardware, das Sie von diesem Hersteller erworben haben, wird abgedeckt, selbst der PC der Sekretärin, auf dem nichtkritische Aufgaben erfüllt werden.

Muss für diesen PC *wirklich* jemand 24/7 vor-Ort zur Verfügung stehen? Die Sekretärin arbeitet täglich von 9:00 Uhr bis 17:00 Uhr Es ist daher relativ unwahrscheinlich, dass:

- Der PC zwischen 17:00 Uhr und 9:00 Uhr genutzt wird (oder am Wochenende)
- Dass ein Ausfall außerhalb der Bürozeiten bemerkt wird (zwischen 9:00 Uhr und 17:00 Uhr)

Es ist daher eine Geldverschwendung, wenn man dafür zahlt, dass dieser PC an einem Samstag mitten in der Nacht gewartet werden kann.

Sie sollten die Service-Vereinbarung aufteilen, sodass nicht-kritische Hardware separat von kritischer Hardware aufgeführt wird. Auf diese Weise können Sie die Kosten so gering als möglich halten.

Anmerkung

Wenn Sie über 20 identische Server verfügen, die für Ihr Unternehmen kritisch sind, sind Sie vielleicht versucht, eine hochrangige Servicevereinbarung für nur einen oder zwei Server abzuschließen und den Rest mit einer kostengünstigeren Vereinbarung abzudecken. Wenn dann irgendeiner der Server ausfällt, behaupten Sie einfach, dass *dieser* derjenige mit dem High-Level Service war.

Sehen Sie davon lieber ab. Es ist nicht nur unehrlich, sondern behalten die meisten Hersteller auch einen guten Überblick über Seriennummern. Selbst wenn Sie einen Weg finden, solche Prüfungen zu umgehen, werden Sie langfristig wesentlich mehr Geld ausgeben, sollten Sie dabei erwischt werden, als wenn Sie ehrlich für die Services, die Sie benötigen, bezahlen.

8.1.2. Software-Ausfälle

Software-Ausfälle können in langer Downtime resultieren. So haben zum Beispiel die Besitzer einer bestimmten Marke von Computersystemen, die für ihre Hochverfügbarkeitsfeatures bekannt sind, dies an eigenem Leibe erfahren. Ein Fehler im Time-Handling-Code des Betriebssystems resultierte darin, dass die Systeme aller Kunden zu einem bestimmten Zeitpunkt jeden Tag abstürzten. Während diese Situation ein eher seltenes Beispiel von Softwarefehlern in Aktion ist, sind andere Software-bezogene Ausfälle vielleicht weniger dramatisch, jedoch genauso zerstörend.

Software-Ausfälle können in einem der folgenden Bereiche zuschlagen:

- Betriebssystem
- Applikationen

Jede Ausfallart hat ihren eigenen speziellen Effekt und wird in den folgenden Abschnitten im Detail dargestellt.

8.1.2.1. Ausfälle des Betriebssystems

Bei dieser Ausfallart ist das Betriebssystem für die Unterbrechung des Services verantwortlich. Ausfälle des Betriebssystems entstehen aus zwei Bereichen:

- Abstürze
- Aufhängen

Das Wichtigste, was Sie über Ausfälle des Betriebssystems wissen sollten, ist, dass alles, was zum Zeitpunkt des Ausfalls läuft, mit abstürzt. Als solches können Systemausfälle extreme Auswirkungen auf die Produktion haben.

8.1.2.1.1. Abstürze

Abstürze treten dann auf, wenn das Betriebssystem einen Fehlerzustand erleidet, von dem es sich nicht erholt. Die Gründe für Abstürze reichen von der Unfähigkeit, ein tieferliegendes Hardwareproblem zu lösen bis hin zu Bugs im Kernel-Code, die das Betriebssystem kompromittieren. Stürzt ein Betriebssystem ab, so muss das System neu gebootet werden, um mit der Produktion fortfahren zu können.

8.1.2.1.2. Aufhängen

Stoppt das Betriebssystem das Bearbeiten von System-Events, kommt das gesamte System zum Stillstand. Dies ist als *Aufhängen* bekannt. Dies kann durch *Deadlocks* (zwei Verbraucher von Ressourcen, die sich im Disput um die Ressource des jeweils anderen befinden) und *Livelocks* (zwei oder mehr Prozesse reagieren auf die Aktivitäten des jeweils anderen, produzieren aber dabei nichts Sinnvolles) entstehen. Das Endresultat ist jedenfalls das Gleiche — ein völliger Produktivitätsausfall.

8.1.2.2. Ausfälle von Applikationen

Im Gegensatz zu Ausfällen des Betriebssystems sind Applikationsausfälle etwas begrenzter im angerichteten Schaden. Abhängig von der jeweiligen Applikation betrifft ein Applikationsausfall eventuell nur eine Person. Ist jedoch eine Server-Applikation davon betroffen, so sind die Konsequenzen eines Ausfalls wesentlich weitreichender.

Applikationsausfälle sowie auch Ausfälle des Betriebsystems können durch Aufhängen oder Abstürzen verursacht werden. Der einzige Unterschied ist, dass hier nur die Applikation sich aufhängt oder abstürzt.

8.1.2.3. Hilfe — Software Support

Genauso wie Hardware-Hersteller Support für ihre Produkte liefern, bieten auch viele Software-Hersteller ihren Kunden Support-Pakete an. Abgesehen von den offensichtlichen Unterschieden (es wird keine Ersatz-Hardware benötigt und die Arbeit kann von Support-Personal über das Telefon aus durchgeführt werden), ähneln Software-Supportverträge denen von Hardware erheblich.

Der jeweilige Support-Level ist von Hersteller zu Hersteller verschieden. Im folgenden finden Sie die häufigeren Support-Strategien:

- Dokumentation
- Selbsthilfe
- Web- oder E-Mail-Support
- Telefon-Support
- Vor-Ort-Support

Jede Art von Support wird in den folgenden Abschnitten genauer beschrieben.

8.1.2.3.1. Dokumentation

Wenn auch meistens übersehen, kann eine Software-Dokumentation als 1-A-Supporttool dienen. Ob Online oder gedruckt, Dokumentation enthält häufig die für eine Problemlösung wichtigen Informationen.

8.1.2.3.2. Selbsthilfe

Selbsthilfe bedeutet, dass der Kunde Online-Ressourcen für die Problemlösung zur Hilfe nimmt. Häufig werden diese Online-Ressourcen als web-basierte FAQ (häufig gestellte Fragen) oder Wissensdatenbanken zur Verfügung gestellt.

FAQs haben meistens nur geringe oder gar keine Auswahlmöglichkeiten, so dass der Kunde sich von Frage zu Frage klicken muss, in der Hoffnung, eine Lösung zu seinem Problem irgendwo zu finden. Knowledgebases (Wissensdatenbanken) sind häufig etwas weiter entwickelt und bieten eine Suche

nach Begriffen. Knowledgebases können in einigen Fällen auch sehr umfangreich sein, was sie zu einem sehr guten Tool für die Problemlösung machen.

8.1.2.3.3. Web- oder E-Mail-Support

Auf vielen Selbsthilfe-Webseiten finden sich auch web-basierte Formulare oder E-Mail-Adressen, über die Sie Ihre Fragen an Mitarbeiter des Supports senden können. Während dies auf den ersten Blick als Verbesserung einer guten Selbsthilfe-Webseite erscheint, hängt es in Wirklichkeit erheblich von denjenigen ab, die die E-Mails beantworten.

Sind die Support-Mitarbeiter überlastet, erweist es sich als schwierig, die nötigen Informationen zu bekommen, da das Hauptaugenmerk auf einer schnellen Beantwortung jeder E-Mail liegt. Der Grund dafür ist, dass fast das gesamte Support-Personal auf Basis der gelösten Probleme evaluiert wird. Eine Eskalation von Problemen ist auch schwierig, da innerhalb einer E-Mail wenig für eine angemessene und hilfreiche Antwort getan werden kann — insbesondere, wenn die Person, die Ihre E-Mail liest, unter Zeitdruck steht.

Den besten Service erhalten Sie, wenn Sie in Ihrer E-Mail alle Fragen ansprechen, die ein Support-Techniker stellen würde. Zum Beispiel:

- Beschreiben Sie klar und deutlich das Problem
- Geben Sie alle wichtigen Versionsnummern an
- Beschreiben Sie, was Sie bereits versucht haben, um das Problem zu lösen (Anwenden der neuesten Patches, Reboot mit Minimalkonfiguration etc.)

In dem Sie dem Support-Techniker diese Informationen geben, haben Sie eine höhere Chance, den benötigten Support zu erhalten.

8.1.2.3.4. Telefon-Support

Wie der Name schon sagt, beinhaltet der Telefon-Support die telefonische Unterstützung eines Technikers. Diese Art von Support ist dem Hardware-Support am ähnlichsten. Es gibt verschiedene Support-Level (mit verschiedenen Abdeckungsstunden, Reaktionszeiten etc.).

8.1.2.3.5. Vor-Ort-Support

Diese auch als On-Site Consulting bekannte Art ist der teuerste Software-Support. Gewöhnlich wird dies nur für das Lösen ganz bestimmter Probleme, wie einer erstmaligen Softwareinstallation und Konfiguration, für bedeutende Upgrades, usw. reserviert. Wie bereits erwähnt, ist dies der teuerste Support.

Es gibt jedoch Vorfälle, wo der vor-Ort-Support sinnvoll ist. Denken Sie zum Beispiel an eine kleinere Firma mit nur einem Systemadministrator. Die Firma will nun ihren ersten Datenbank-Server einsetzen, aber der Einsatz (und die Verwaltung) ist nicht umfassend genug, um einen eigenen Datenbank-Administrator zu rechtfertigen. In dieser Situation kann es durchaus günstiger sein, einen Experten des Datenbankherstellers in die Firma zu holen, der den anfänglichen Einsatz (und je nach Bedarf zu einem späteren Zeitpunkt) regelt, als den Systemadministrator im Umgang mit der Software zu schulen.

8.1.3. Ausfälle der Umgebung

Auch wenn die Hardware ordnungsgemäß läuft und die Software richtig konfiguriert ist und ordnungsgemäß funktioniert, können trotzdem noch Probleme auftreten. Die häufigsten Probleme, die außerhalb des Systems selbst auftreten, haben mit der physikalischen Umgebung, in der sich das System befindet, zu tun.

Umgebungsprobleme können in vier Hauptkategorien aufgeteilt werden:

- Intaktheit des Gebäudes
- Elektrizität
- Klimaanlage
- Das Wetter und die Außenwelt

8.1.3.1. Gebäudeintegrität

Angesichts einer derart einfachen Grundstruktur, erfüllt ein Gebäude eine enorme Anzahl an Funktionen. Es bietet Schutz vor den Naturgewalten. Es bietet das richtige Mikro-Klima für alles, das sich im Gebäude befindet. Es besitzt Mechanismen für die Bereitstellung von Strom und Schutz vor Feuer, Diebstahl und Vandalismus. Daher ist es auch nicht verwunderlich, dass einiges in Bezug auf Gebäude schiefgehen kann. Hier sind einige Dinge:

- Das Dach kann undicht werden und somit Wasser in Datenzentren eindringen.
- Verschiedene Systeme im Gebäude (z.B. Wasser, Abwasser oder Luft) können ausfallen und das Gebäude unbewohnbar machen.
- Fußböden können evtl. nicht die Last Ihrer Einrichtung im Datenzentrum tragen.

Eine lebendige Vorstellungskraft ist wichtig, wenn es darum geht, was bei Gebäuden alles schiefgehen kann. Die obige Liste ist ist nur der Anfang, um Sie in die richtige Richtung zu weisen.

8.1.3.2. Elektrizität

Da Strom die Lebensquelle für jedes Computersystem ist, sind Strom-bezogene Angelegenheiten von höchster Bedeutung für den Systemadministrator. Es sind mehrere Aspekte zu betrachten, welche in den folgenden Abschnitten eingehender beschrieben werden.

8.1.3.2.1. Die Sicherheit Ihrer Elektrizität.

Als erstes muss festgestellt werden, wie sicher Ihre reguläre Stromversorgung ist. Wie wahrscheinlich jedes andere Datencenter auch, erhalten Sie Ihren Strom von einem örtlichen Energieversorgungsunternehmen über Elektrizitätsleitungen. Hierdurch sind Sie in der Sicherung Ihrer primären Stromversorgung eingeschränkt.

Tipp

Unternehmen, die sich im Grenzbereich eines Energieunternehmens befinden, können unter Umständen einen Anschluss an zwei verschiedene Energienetze aushandeln:

- Das eine, das Ihren Bezirk speist
- Das andere vom benachbarten energieerzeugenden Unternehmen

> Die Kosten einer Stromleitung von einem benachbarten Netz sind beträchtlich. Daher kommt diese Option wahrscheinlich nur für größere Unternehmen in Frage. Diese Unternehmen werden jedoch feststellen, dass die Vorteile durch zusätzliche Stromversorgung die Kosten vielfach überwiegen.

Die Hauptpunkte, die es zu prüfen gilt, sind die Wege, auf die der Strom auf das Gelände und in die Gebäude Ihrer Firma kommt. Sind die Elektrizätsleitungen über oder unter der Erde? Überirdische Leitungen sind anfällig für:

- Schäden durch extremes Wetter (Eis, Wind, Blitzschlag)
- Verkehrsunfälle, bei denen die Masten und/oder Transformatoren beschädigen
- Tiere, die zur falschen Zeit am falschen Ort sind und die Leitungen kurzschließen

Unterirdische Leitungen haben jedoch auch ganz besondere Probleme:

- Schäden durch Bauarbeiter, die am falschen Ort graben
- Überflutungen
- Blitzschlag (jedoch weniger anfällig als überirdische Leitungen)

Verfolgen Sie nun die Leitungen bis zu Ihrem Gebäude. Werden diese erst über einen externen Transformator geleitet? Ist dieser Transformator vor Fahrzeugen oder umfallenden Bäumen geschützt? Sind alle offenliegenden Schalter vor unbefugter Benutzung geschützt?

Können diese Leitungen (oder Kabelführungen) innerhalb des Gebäudes anderen Problemen ausgesetzt sein? Könnte zum Beispiel ein Wasserrohrbruch den Maschinenraum überfluten?

Verfolgen Sie die Leitung ins Datencenter. Gibt es irgendetwas, das unvorhergesehen die Stromversorgung unterbrechen könnte? Teilt sich zum Beispiel das Datencenter einen oder mehrere Stromkreise mit Nicht-Datencenter-Verbrauchern? Ist dies der Fall, kann eines Tages vielleicht die externe Last den Überlastungsschutz des Schaltkreises auslösen und im Zuge dessen das Datenzentrum ohne Strom belassen.

8.1.3.2.2. Stromqualität

Das alleinige Sicherstellen, dass die Energiequellen für das Datenzentrum sicher sind, reicht leider nicht aus. Sie müssen auch an die Qualität der Energie, die zum Datencenter geliefert wird, denken. Sie sollten mehrere Faktoren in Betracht ziehen:

Spannung

> Die hereinkommende Spannung muss konstant sein und darf keine negativen Spannungsspitzen (auch *Spannungsabfall* genannt) oder positiven Spannungsspitzen (auch bekannt als *Stromspitzen*) aufweisen.

Wellenform

> Es muss eine saubere Sinuswelle mit einer nur minimalen *THD* (Total Harmonic Distortion - Harmonische Verzerrung) sein.

Frequenz

> Die Frequenz muss stabil sein (die meisten Länder verwenden eine Frequenz von 50Hz oder 60 Hz).

Störungen

Es dürfen keine *RFI* (Radio Frequency Interference - Funkstörungen) oder *EMÜ* (Elektormagnetische Überlagerungen) vorkommen.

Stromstärke

Es muss ein bestimmter Nennstrom, der für den Betrieb des Datencenters ausreicht, geliefert werden.

Der direkt vom Energieversorgunsgunternehmen gelieferte Strom entspricht normalerweise nicht dem für ein Datenzentrum nötigen Standard. Es wird daher ein gewisser Grad an Stromwandlung benötigt. Es gibt hierfür verschiedene Methoden:

Überspannungsschutz

Ein Überspannungsschutz tut genau das, was der Name bereits sagt — Überspannungen aus der Stromversorgung herausfiltern. Die meisten Überspannungsschutz-Einrichtungen tun nichts anderes und die Ausrüstung bleibt anfällig für andere Energie-bezogene Probleme.

Power-Conditioner

Power-Conditioner folgen einem eher ganzheitlicheren Ansatz. Abhängig von der technischen Raffinesse der Einheit können Stromanlagen die meisten oben beschriebenen Probleme lösen.

Motor-Generator-Sätze

Ein Motor-Generator-Satz ist im wesentlichen ein großer Elektromotor, der von Ihrer normalen Stromversorgung angetrieben wird. Der Motor ist mit einem Schwungrad verbunden, das wiederum mit einem Generator verbunden ist. Der Motor treibt das Schwungrad und den Generator an, der dann genügend Strom für das Datencenter erzeugt. Auf diese Weise ist das Datencenter elektrisch gesehen vom externen Strom isoliert, was wiederum die meisten Strom-bezogenen Probleme eliminiert. Das Schwungrad liefert auch eine Stromversorgung durch kurze Stromausfälle hinweg, da es mehrere Sekunden dauert, bis das Schwungrad so langsam wird, dass kein Strom mehr erzeugt werden kann.

Unterbrechungsfreie Stromversorgung

Einige Typen unterbrechungsfreier Stromversorgung (allgemein auch als *UPS* bekannt) enthalten fast alle (wenn nicht alle) der Schutzeigenschaften eines Power Conditioners[2].

Mit den letzten beiden Technologien gehen wir zu einem Thema über, an das die meisten denken, wenn es um Strom geht — Backup-Strom. Im nächsten Abschnitt werden verschiedene Ansätze für Backup-Strom beschrieben.

8.1.3.2.3. Backup-Strom

Ein Begriff, den wohl die meisten schon gehört haben, ist *Stromausfall*. Ein Stromausfall oder Blackout ist der vollständige Verlust elektrischer Stromversorgung und kann von Sekundenbruchteilen bis hin zu Wochen dauern.

Dadurch, dass die Dauer von Stromausfällen so verschieden ist, ist es wichtig, Backup-Strom mittels verschiedender Technologien für verschieden lange Ausfälle bereitzustellen.

2. UPS Technologie wird eingehender behandelt in Abschnitt 8.1.3.2.3.2.

Tipp

Die häufigsten Stromausfälle dauern im Durchschnitt nur wenige Sekunden. Längere Ausfälle sind wesentlich seltener. Konzentrieren Sie sich deshalb als erstes auf Stromausfälle mit einer Dauer von wenigen Minuten und arbeiten Sie danach Methoden für Ausfälle längere Dauer aus.

8.1.3.2.3.1. Energieversorgung für die nächsten paar Sekunden

Da die meisten Stromausfälle nur ein paar Sekunden dauern, muss Ihre Backup-Lösung zwei Hauptcharakteristika aufweisen:

- Sehr kurze Umschaltzeit zum Backup-Strom (bekannt als *Transferzeit*)
- Eine *Laufzeit* (die Zeit, für die Backup-Strom geliefert wird) gemessen in Sekunden bis Minuten

Die Backup-Strom Lösungen, die diesen Charakteristika entsprechen, sind Motor-Generator-Sätze und USVs. Das Schwungrad im Motor-Generator-Satz ermöglicht dem Generator, kontinuierlich Strom zu produzieren, um einen Stromausfall von etwa einer Sekunde zu überbrücken. Motor-Generator-Sätze sind relativ sperrig und kostspielig und stellen somit eher eine Lösung für mittelgroße und größere Datencenter dar.

Eine andere Technologie — USV genannt — kann jedoch in den Situationen einspringen, in denen ein Motor-Generator-Satz zu kostspielig wird. Es kann auch längere Ausfälle überbrücken.

8.1.3.2.3.2. Strom für die nächsten paar Minuten bereitstellen

USVs sind in verschiedenen Größen erhältlich — von kleinen für den Betrieb eines einzelnen PCs für fünf Minuten oder auch für die Stromversorgung eines gesamten Datencenters für eine Stunde oder länger.

USVs bestehen aus den folgenden Komponenten:

- Ein *Transfer-Schalter* für das Umschalten der primären Stromversorgung zur Backup-Stromversorgung.
- Eine Batterie für Backup-Energie
- Ein*Wechselrichter*, der den Gleichstrom der Batterie in den Wechselstrom, der von der Datencenter-Hardware benötigt wird, umwandelt.

Abgesehen von der Größe und Batteriekapazität der Einheit werden USVs in zwei Grundausstattungen geliefert:

- Eine *Offline*-USV verwendet Wechselrichter, um Strom nur dann zu erzeugen, wenn die Primär-Stromquelle ausfällt.
- Eine *Online*-USV verwendet Wechselrichter, um ständig Strom zu erzeugen und speist nur dann den Wechselrichter durch ihre Batterie, wenn die Primär-Stromquelle ausfällt.

Jeder Typ hat seine Vor- und Nachteile. Eine Offline-USV ist generell etwas kostengünstiger, da der Wechselrichter nicht für Vollzeitbetrieb ausgelegt sein muss. Probleme mit dem Wechselrichter werden jedoch meistens nicht rechtzeitig erkannt (spätestens beim nächsten Stromausfall).

Online-USVs sind im allgemeinen besser bei der Bereitstellung von sauberem Strom, da eine Online-USV Vollzeit Strom für Sie erzeugt.

Egal welche Art USV Sie einsetzen, die USV muss auf die zu erwartende Last angepasst werden so dass die USV genügend Kapazität zur Elektrizitätserzeugung mit benötigtem Strom und Spannung hat), *und* es muss festgestellt werden, wie lange das Datencenter im Batteriebetrieb laufen soll.

Dazu müssen Sie als erstes die Lasten festlegen, die von der USV gespeist werden sollen. Bestimmen Sie für jede Hardwarekomponente, wieviel Strom benötigt wird (steht meistens auf einem Schild in der Nähe des Stromkabels). Notieren Sie die Spannung (Volt), Leistung (Watt) und/oder Strom (Ampere). Sobald Sie alle diese Daten für die Hardware haben, müssen Sie diese in *VA* (Volt-Ampere) umwandeln. Haben Sie eine Zahl in Watt, können Sie diese als VA nehmen. Haben Sie Ampere, müssen Sie diese mit Volt multiplizieren, um die VA zu erhalten. Wenn Sie nun die VA-Werte addieren, erhalten Sie die VA-Leistung, die für das UVS benötigt wird.

Anmerkung

Genaugenommen ist dieser Ansatz für die Berechnung des VA nicht richtig; für den echten VA-Wert müssten Sie den Leistungsfaktor für jede Einheit kennen, und diese Information wird selten wenn überhaupt bereitgestellt. Die auf dem hier beschriebenen Wege berechneten Werte reflektieren den schlimmsten anzunehmenden Wert und lässt somit etwas Luft für etwas erhöhte Sicherheit.

Das Bestimmen der Laufzeit ist eher eine geschäftliche als eine technische Frage — gegen welche Art Ausfälle wollen Sie sich schützen und wieviel wollen Sie dafür ausgeben? Die meisten wählen Laufzeiten von weniger als einer Stunde oder maximal zwei Stunden, da danach Batterieenergie sehr kostspielig wird.

8.1.3.2.3.3. Bereitstellen von Energie für die nächsten paar Stunden (und darüber hinaus)

Sobald Stromausfälle in Tagen gemessen werden müssen, wird die Auswahl noch wesentlich teurer. Technologien, die langfristige Stromausfälle überbrücken können, sind auf Generatoren, die von einem Motor angetrieben werden, beschränkt — hauptsächlich Diesel- und Gasturbinen.

Anmerkung

Bitte beachten Sie, dass motorgetriebene Generatoren regelmäßiges Auffüllen des Treibstoffs benötigen. Sie sollten die Verbrennungsrate Ihres Generators bei Maximalbelastung kennen und entsprechend Kraftstofffüllungen arrangieren.

An dieser Stelle sind Ihre Optionen offen, vorausgesetzt, Ihr Unternehmen hat ausreichend finanzielle Ressourcen. Dies ist auch ein Bereich für den Experten die beste Lösung für Ihr Unternehmen festlegen können. Es haben nur ganz wenige Systemadministratoren das spezielle Wissen, das nötig ist, um die Beschaffung und den Einsatz dieser Art von Stromerzeugungssystemen zu planen.

Tipp

Tragbare Generatoren aller Größen können gemietet werden und machen es so möglich, die Vorteile eines Generators zu genießen, ohne die Summen für eine Anschaffung dieser Aufbringen zu müssen. Behalten Sie jedoch im Hinterkopf, dass wenn eine Katastrophe in Ihrer allgemeinen Umgebung eintritt, gemietete Generatoren rar und teuer werden.

8.1.3.2.4. Planung für langfristige Stromausfälle

Während ein 5-minütiger Stromausfall nicht mehr als unangenehm für das Personal in einem dunklen Büro ist, wie sieht es dagegen mit einem Ausfall über eine Stunde aus? 5 Stunden? Ein Tag? Eine Woche?

Tatsache ist, dass irgendwann, auch wenn das Datencenter normal funktioniert, ein längerdauernder Ausfall Ihr Unternehmen treffen wird. Betrachten Sie die folgenden Punkte:

- Was passiert, wenn es keinen Strom gibt, um das Klima im Datencenter aufrecht zu erhalten?
- Was passiert, wenn es keinen Strom gibt, um das Klima im gesamten Gebäude aufrecht zu erhalten?
- Was passiert, wenn es keinen Strom gibt, um Workstations, die Telefonanlage oder das Licht zu betreiben?

Der Punkt hier ist, dass Ihr Unternehmen festlegen muss, zu welchem Zeitpunkt ein Stromausfall einfach hingenommen werden muss. Ist dies keine Option, sollte Ihr Unternehmen überlegen, wie es vollkommen unabhängig für längere Zeiträume funktionieren kann, was bedeutet, dass sehr große Generatoren zur Versorgung des gesamten Gebäudes benötigt werden.

Natürlich kann diese Planung nicht in einem totalen Vakuum stattfinden. Es ist ziemlich wahrscheinlich, dass was auch immer den längeren Stromausfall verursacht, auch die Welt um Sie herum betrifft und dieser Umstand auch Ihr Unternehmen beeinflusst; auch wenn unbegrenzter Ersatzstrom vorhanden ist.

8.1.3.3. Heizung, Lüftung und Klimaanlage

Die Heizungs-, Lüftungs- und Klimatisierungssysteme (*HLK*), die in modernen Bürogebäuden eingesetzt werden, sind unwahrscheinlich weit entwickelt. Häufig durch Computer gesteuert sind HLK-Systeme wichtig für das Bereitstellen eines angenehmen Arbeitsklimas.

Datencenter haben häufig zusätzliche Lüftungsanlagen, hauptsächlich um die von vielen Computern und anderen Geräten erzeugte Wärme abzuleiten. Ausfälle in einem HLK-System können die Fortsetzung des Betriebs eines Datencenters verhindern. Durch die Komplexität und elektro-mechanische Natur sind die Möglichkeiten eines Ausfalls reichhaltig und divers. Hier ein paar Beispiele:

- Die Lüftungsanlagen (im wesentlichen große Ventilatoren, angetrieben von großen Elektro-Motoren) können durch eine elektrische Überlastung, Lagerausfall, Keilriemenriss etc. ausfallen
- Die Kühleinheiten (auch *Chillers* genannt) können ihr Kühlmittel durch Lecks verlieren oder die Motoren oder Kompressoren können klemmen.

HLK-Reparaturen und Wartung ist ein spezialisierter Bereich — ein Bereich, den der normale Systemadministrator Experten überlassen sollte. Ein Systemadministrator sollte zumindest jedoch sicherstellen, dass die HLK-Ausrüstung täglich (oder mehrmals täglich) auf normalen Betrieb geprüft und nach den Richtlinien des Herstellers gewartet wird.

8.1.3.4. Das Wetter und die Außenwelt

Es gibt einige Arten von Wetter, die einem Systemadministrator Probleme bereiten können.

- Schnee und Eis können Mitarbeiter des Datencenters davon abhalten, zur Arbeit zu kommen und Kondensatoren der Kimaanlagen verstopfen, was erhöhte Temperaturen im Datencenter zur Folge hat. Und dann womöglich niemand dort ist, der etwas dagegen unternehmen kann.

- Stürme können Strom und Kommunikation unterbrechen, und sehr starke Stürme das Gebäude selbst beschädigen.

Andere Arten von Wetter können weitere Probleme verursachen, auch wenn diese nicht ganz so häufig sind. Sehr hohe Temperaturen zum Beispiel können zu überlasteten Kühlsystemen führen und im Zuge dessen zu Stromausfällen, wenn das örtliche Stromnetz überlastet wird.

Auch wenn man nicht viel am Wetter ändern kann, ist jedoch das Wissen, inwiefern dies den Betrieb Ihres Datencenters beeinflussen kann, wichtig für das Aufrechterhalten des Betriebes, auch bei schlechtem Wetter.

8.1.4. Menschliches Versagen

Man sagt, dass Computer *wirklich* perfekt sind. Der Grund für diese Aussage ist, dass wenn man nur lange genug sucht, hinter jedem Computerfehler einen menschlichen Fehler findet, der diesen verursacht. In diesem Abschnitt werden die allgemeineren Typen menschlichen Versagens und deren Auswirkungen untersucht.

8.1.4.1. Fehler des Endbenutzers

Die Benutzer eines Computers können Fehler machen, die bedeutende Auswirkungen haben. Durch ein allgemein unprivilegiertes Betriebssystem sind Benutzerfehler meistens beschränkt. Da die meisten Benutzer mit einem Computer über eine oder mehrere Applikationen kommunizieren, treten die meisten Fehler innerhalb dieser Applikationen auf.

8.1.4.1.1. Unsachgemäße Verwendung von Applikationen

Wenn Applikationen nicht ordnungsgemäß verwendet werden, können verschiedene Probleme auftreten:

- Dateien, die unbeabsichtigt überschrieben wurden
- Falsche Daten, die als Eingabe für eine Applikation verwendet wurden
- Dateien, die nicht eindeutig benannt und organisiert wurden
- Daten, die versehentlich gelöscht wurden

Die Liste könnte noch weiter gehen, reicht an diesem Punkt jedoch völlig für Anschauungszwecke aus. Dadurch, dass Benutzer keine Superuser-Privilegien haben, beschränken sich die Fehler meistens auf deren eigene Dateien. Aus diesem Grund ist der beste Ansatz zweigleisig:

- Lehren Sie Benutzern den richtigen Umgang mit Applikationen und richtige Dateimanagement-Techniken
- Stellen Sie sicher, dass regelmäßig Backups der Benutzerdaten durchgeführt werden und dass der Wiederherstellungsprozess so gestrafft und schnell wie möglich vonstatten geht.

Darüberhinaus kann nur wenig getan werden, um Benutzerfehler auf ein Minimum zu beschränken.

8.1.4.2. Fehler des Bedienungspersonals

Bediener haben eine engere Beziehung mit den Rechnern in einem Unternehmen als Endbenutzer. Endbenutzer-Fehler sind eher auf Applikationen bezogen, während Bediener eine weitere Bandbreite von Aufgaben durchführen. Auch wenn die Art der Aufgabe von anderen vorgegeben wurde, können einige dieser Aufgaben die Verwendung von Utilities auf Systemebene miteinschließen. Die Arten von

Fehlern, die ein Bediener machen kann, konzentrieren sich auf die Fähigkeit des Bedieners, bestimmte Verfahrensweisen einzuhalten.

8.1.4.2.1. Nichteinhalten von Verfahrensweisen

Bediener sollten einen dokumentierten und verfügbaren Satz an Verfahrensweisen für beinahe alle durchzuführenden Aktionen haben [3]. Es kann vorkommen, dass ein Bediener den Richtlinien nicht 100prozentig folgt. Hierfür kann es verschiedene Gründe geben:

- Die Umgebung wurde irgendwann geändert, die Prozeduren jedoch nicht aktualisiert. Nun ändert sich die Umgebung wieder, was die Verfahrensweise im Kopf des Bedieners ungültig werden lässt. Auch wenn jetzt die Verfahrensweisen aktualisiert werden (was relativ unwahrscheinlich ist, da diese auch vorher nicht aktualisiert wurden), ist dies dem Bediener höchstwahrscheinlich nicht bewusst.
- Die Umgebung wurde geändert und es gibt keine bestimmten Verfahrensweisen. Dies ist so gesehen nur eine noch unkontrollierbarere Version der vorher beschriebenen Situation.
- Es gibt Vorgehensweisen, der Bediener will oder kann jedoch diesen nicht folgen.

Abhängig von der Managementstruktur in Ihrem Unternehmen können Sie unter Umständen nicht mehr dazu beitragen, als Ihre Bedenken dem zuständigen Manager mitzuteilen. In jedem Fall können Sie Ihre Hilfe bei der Lösung des Problems anbieten

8.1.4.2.2. Fehler, die innerhalb bestimmter Vorgehensweisen gemacht werden

Auch wenn der Bediener sich genauestens an die Verfahrensweise hält und diese Prozeduren korrekt sind, können trotzdem Fehler auftreten. Ist dies der Fall, kann es sein, dass der Bediener nicht sorgfältig genug arbeitet (dann sollte das Management eingeschaltet werden).

Es kann auch ein einmaliger Fehler sein. In diesem Fall bemerkt ein geübter Bediener, dass irgendetwas nicht stimmt und sucht Hilfe. Ermutigen Sie die Bediener, die jeweilig Zuständigen zu kontaktieren, sollte etwas nicht richtig erscheinen. Auch wenn viele Bediener hoch-qualifiziert und in der Lage sind, viele Probleme selbst zu lösen, ist es jedoch eine Tatsache, dass dies nicht in deren Aufgabenbereich fällt. Und ein Problem, das durch einen gutgemeinten Versuch eines Bedieners lediglich schlimmer gemacht wurde, wirk sich nicht nur negativ auf den Bediener selbst aus, sondern auch auf Ihre Fähigkeit, ein eventuell anfänglich kleines Problem rasch zu lösen.

8.1.4.3. Fehler von Systemadministratoren

Im Gegensatz zu Bedienern erfüllen Systemadministratoren eine große Reihe von Aufgaben mittels Computern. Desweiteren basieren die Aufgaben, die von Systemadministratoren durchgeführt werden, meistens nicht auf dokumentierten Vorgehensweisen.

Aus diesem Grund schaffen sich Systemadministratoren manchmal zusätzliche Arbeit, wenn diese nicht sorgfältig genug arbeiten. Im Laufe der täglichen Arbeit haben Systemadministratoren genügend Zugang zu Systemen (und nicht zu vergessen Super-User Berechtigungen), um diese aus Versehen zum Absturz zu bringen.

Systemadministratoren unterlaufen dabei entweder Konfigurationsfehler oder Fehler während der Wartung.

---

3. Bestehen keine gültigen Richtlinien zum Thema Verfahrensweisen in Ihrem Unternehmen, arbeiten Sie am besten mit den Bedienern selbst, dem Management und den Endbenutzern zusammen, um solche zu erstellen. Ohne gewisse Richtlinien ist ein Datencenter im wahrsten Sinne des Wortes außer Kontrolle. Früher oder später ist das Auftreten schwerwiegender Probleme höchstwahrscheinlich.

8.1.4.3.1. Konfigurationsfehler

Systemadministratoren müssen häufig verschiedene Aspekte eines Computersystems konfigurieren. Dies umfasst:

- E-Mail
- Benutzer-Accounts
- Netzwerk
- Applikationen

Die Liste kann so noch eine Weile weitergehen. Die eigentliche Aufgabe beim Konfigurieren variiert. Für einige Aufgaben müssen große Textdateien bearbeitet werden (mit einer von hunderten verschiedener Konfigurationsdatei-Syntaxen) während für andere eine Konfigurations-Utility benötigt wird.

Die Tatsache, dass alle diese Aufgaben unterschiedlich gehandhabt werden, ist nur noch eine zusätzliche Herausforderung zur eigentlichen Tatsache, dass jede Konfigurationsaufgabe eine andere Art von Wissen voraussetzt. So unterscheidet sich z.B. das Wissen, das zur Konfiguration eines Mail-Transport-Agents erforderlich ist, wesentlich vom Wissen, das zum Konfigurieren einer neuen Netzwerkverbindung notwendig ist.

So gesehen ist es nahezu verwunderlich, dass im Grunde gesehen nur so *wenige* Fehler gemacht werden. Auf jeden Fall ist die Konfiguration eine Herausforderung für Systemadministratoren und wird es wohl auch immer bleiben. Gibt es irgendetwas, was man tun kann, um den gesamten Prozess weniger fehleranfällig zu machen?

8.1.4.3.1.1. Änderungsüberwachung

Der Grundgedanke bei jeder Konfigurationsänderung ist, dass eine gewisse Art von Änderung durchgeführt wird. Diese Änderung kann groß oder auch klein sein, ist aber in jeden Fall eine Änderung und sollte auf bestimmte Art und Weise behandelt werden.

Viele Unternehmen haben eine bestimmte Art von Änderungsüberwachung implementiert. Der Hintergedanke dabei ist, Systemadministratoren (und allen, die von der Änderung betroffenen sind) bei der Durchführung der Änderungen zu helfen und somit das Fehlerrisiko zu minimieren.

Eine Änderungsüberwachung teilt die Änderungen in verschiedene Schritte auf. Hier ein Beispiel:

Vorausgehende Recherche

Eine vorausgehende Recherche versucht Folgendes klar zu definieren:

- Die Art der Änderung, die durchgeführt werden soll
- Die Auswirkungen, falls die Änderung erfolgreich ist
- Einen Plan B, falls die Änderung nicht erfolgreich ist
- Eine Einschätzung, welche Arten von Ausfällen vorkommen könnten

Vorausgehende Forschung kann das Testen der vorgeschlagenen Änderungen in einer geplanten Ausfallzeit sein oder sogar das Implementieren der Änderungen in einer besonderen Test-Umgebung auf dazu bestimmter Test-Hardware.

Planung

Die Änderungen werden in Hinblick auf die eigentliche Implementierung untersucht. Die Planung umfasst die Abfolge und den Zeitpunkt der Änderungen (zusammen mit der Abfolge und dem Zeitpunkt jeglicher Schritte, die nötig werden, sollte ein Problem auftreten) sowie das Sicherstellen, dass die zugewiesene Zeit für die Änderung ausreichend ist und nicht mit anderen Aktivitäten auf Systemebene in Konflikt gerät.

Das Ergebnis dieses Prozesses ist häufig eine Schritt-für-Schritt gegliederte Checkliste für den Systemadministrator. Zusammen mit jedem Schritt werden Anweisungen gegeben, die ausgeführt werden müssen, sollte dieser Schritt fehlschlagen. Es werden auch geschätzte Zeiten angegeben, die einem Systemadministrator das Prüfen erleichtern, ob alles nach Plan läuft.

Ausführung

Zu diesem Zeitpunkt ist die eigentliche Ausführung der Schritte für die Implementierung der Änderungen klar und unmissverständlich. Die Änderungen werden entweder implementiert oder (falls Probleme auftreten) auch nicht implementiert.

Überwachung

Unabhängig davon ob die Änderungen implementiert werden oder nicht, wird die Umgebung überwacht, um sicherzustellen, dass alles richtig funktioniert.

Dokumentation

Wurden die Änderungen implementiert, so wird die bestehende Dokumentation aktualisiert, um die Konfigurationsänderungen zu reflektieren.

Offensichtlich erfordern nicht alle Konfigurationsänderungen diese Detailgenauigkeit. Das Erstellen eines neuen Benutzeraccounts sollte keine vorausgehende Recherche benötigen und das Planen beschränkt sich auf das Festlegen, wann der Systemadministrator einen Moment Zeit hat, um den Account einzurichten. Die Ausführungsdauer ist dementsprechend kurz. Die Überwachung besteht lediglich aus dem Sicherstellen, dass der Account verwendbar ist und die Dokumentation beschränkt sich wahrscheinlich auf das Versenden einer E-Mail an der Manager des neuen Benutzers.

Mit immer komplexer werdenden Konfigurationsänderungen, entsteht auch der Bedarf nach formelleren Änderungsüberwachungs-Prozessen.

8.1.4.3.2. Während der Wartung verursachte Fehler

Diese Art von Fehlern können heimtückisch sein, da die tägliche Wartung selten geplant oder dokumentiert wird.

Systemadministratoren sehen die Ergebnisse dieser Art Fehler jeden Tag, insbesondere von Benutzern, die schwören, nichts geändert zu haben — der Computer ist von ganz alleine kaputtgegangen. Der Benutzer kann sich zumeist nicht daran erinnern, was dieser zuletzt durchgeführt hat. Und wenn Ihnen das gleiche passieren würde, dann könnten Sie sich wahrscheinlich auch nicht mehr daran erinnern.

Wenn Sie in der Lage sein wollen, Probleme schnell zu lösen, so müssen Sie sich immer daran erinnern können, welche Änderungen Sie während der Wartung gemacht haben. Ein "ausgewachsener" Änderungsüberwachungs-Prozess ist eher unrealistisch für die zahllosen kleinen Dinge, die im Laufe des Tages anfallen. Was können Sie nun tun, um die 101 kleinen Dinge, die ein Systemadministrator tagtäglich zu erledigen hat, im Auge zu behalten?

Die Antwort ist einfach — machen Sie Notizen. Machen Sie Notizen, egal ob auf Papier, in einem PDA oder in Form von Kommentaren in den betroffenen Dateien. Indem Sie sich aufschreiben, was Sie getan haben, haben Sie eine bessere Chance, einen Fehler auf eine zum Beispiel kürzlich durchgeführte Änderung zurückzuführen.

8.1.4.4. Fehler des Wartungspersonals

Manchmal machen genau diejenigen, die Ihnen beim zuverlässigen Betrieb Ihrer Systeme helfen sollen, alles noch viel schlimmer. Dies ist keine Verschwörung, sondern liegt im allgemeinen daran, dass irgendjemand, der an irgendeiner Technologie arbeitet, diese auch lahmlegen kann. Bei der Arbeit hat

es den selben Effekt, wenn ein Programmierer zum Beispiel durch das Reparieren eines Bugs einen neuen Bug kreiert.

8.1.4.4.1. Unsachgemäß reparierte Hardware

In diesem Fall konnte ein Techniker entweder das Problem nicht richtig diagnostizieren und hat daraufhin eine unnötige (und unnütze) Reparatur durchgeführt oder die Diagnose war zwar korrekt, die Reparatur wurde jedoch nicht richtig ausgeführt. Es kann zum Beispiel sein, dass das Teil selbst kaputt war oder nicht die richtige Prozedur bei der Reparatur eingehalten wurde.

Aus diesem Grund ist es wichtig, zu jeder Zeit den Überblick zu haben, was der Techniker gerade macht. Dadurch können Sie auf Ausfälle achten, die den Anschein erwecken auf irgendeine Weise mit dem eigentlichen Problem in Verbindung zu stehen. Dies hält auch den Techniker auf dem Laufenden, falls ein Problem auftreten sollte. Ansonsten besteht die Chance, dass der Techniker dieses Problem als neu betrachtet und nicht in Zusammenhang mit dem angeblich bereits reparierten Problem sieht. Auf diese Weise wird keine Zeit mit dem Suchen nach dem falschen Problem verschwendet.

8.1.4.4.2. Beim Lösen eines Problems ein anderes schaffen

Es kann manchmal vorkommen, dass auch wenn ein Problem diagnostiziert und erfolgreich gelöst wurde, ein anderes Problem an dessen Stelle auftaucht. Ein CPU-Modul wurde ersetzt, die Plastikverpackung dessen wurde jedoch im Schrank gelassen, blockiert nun den Lüfter und verursacht einen Ausfall durch Überhitzung. Oder die fehlerhafte Festplatte im RAID-Array wurde ersetzt, da aber versehentlich ein Stecker auf einer anderen Festplatte getrennt wurde, ist das Array weiterhin betriebsunfähig.

Diese Dinge können das Ergebnis chronischer Schlampigkeit oder eines unbeabsichtigten, einmaligen Fehlers sein. Schlussendlich macht es keinen Unterschied. Sie sollten grundsätzlich die Reparaturen eines Technikers sorgfältig prüfen und sicherstellen, dass das System ordnungsgemäß funktioniert, bevor der Techniker Ihr Unternehmen verlässt.

8.2. Backups

Backups haben zwei Hauptzwecke:

- Sie erlauben die Wiederherstellung einzelner Dateien
- Sie erlauben die vollständige Wiederherstellung ganzer Dateisysteme

Der Hauptzweck ist die Grundlage für die typische Dateiwiederherstellung: ein Benutzer löscht aus Versehen eine Datei und fragt, ob diese vom letzten Backup wiederhergestellt werden kann. Die genauen Umstände können variieren, aber dies ist die häufigste Anwendung für Backups.

Die zweite Situation ist der Alptraum eines jeden Systemadministrators: aus irgendeinem Grund hat der Systemadministrator Hardware vor sich, die irgendwann ein produktiver Teil des Datencenters war. Doch jetzt ist dies nur noch ein lebloser Klumpen Stahl und Silikon. Was fehlt, ist die Software und alle Daten, die von Ihnen und den anderen Benutzern über die Jahre gesammelt wurden. Angeblich wurde von allem ein Backup erstellt. Die Frage ist nur: wirklich?

Und wenn dies der Fall ist, sind Sie in der Lage, diese wiederherzustellen?

8.2.1. Verschiedene Daten: Verschiedene Backup-Ansprüche

Schauen Sie sich die Art von Daten an,[4] die von einem normalen Computersystem verarbeitet und gespeichert werden. Sie werden feststellen, dass einige Daten sich so gut wie nie ändern und andere ständig im Wandel begriffen sind.

Die Geschwindigkeit, mit der sich die Daten ändern, ist maßgebend für das Design eine Backups. Hierfür gibt es zwei Gründe:

- Ein Backup ist nichts weiter als ein Schnappschuss der Daten, für die ein Backup durchgeführt wird. Es ist eine Reflektion der Daten zu einem bestimmten Zeitpunkt.
- Daten, die sich eher unregelmäßig ändern, brauchen auch nur unregelmäßig gesichert werden. Daten, die sich häufig ändern, müssen auch häufiger gesichert werden.

Systemadministratoren, die ein gutes Allgemeinverständnis ihrer Systeme, Benutzer und Applikationen haben, sind auch schnell in der Lage, die Daten auf ihren Systemen in verschiedene Kategorien einzuteilen. Hier sind einige Beispiele:

Betriebssystem

Diese Daten ändern sich normalerweise nur während Aktualisierungen, Installationen von Bug Fixes und jeglichen bestimmten Änderungen.

Tipp

Sollten Sie überhaupt Backups von einem Betriebssystem durchführen? Dies ist eine Frage, über der sich viele Systemadministratoren den Kopf zerbrochen haben. Auf der einen Seite ist eine Neuinstallation eines Betriebssystems eine Option, vorausgesetzt der Installationsprozess ist relativ unkompliziert und die Applikationen der Bug Fixes und angepassten Software sind gut dokumentiert und leicht reproduzierbar.

Auf der anderen Seite ist ein Backup des Betriebssystems die richtige Wahl, wenn Zweifel bestehen, dass eine Neuinstallation die ursprüngliche Systemumgebung vollständig wiederherstellen kann. Diese Backups müssen nicht so häufig wie die Backups für Produktionsdaten durchgeführt werden. Gelegentliche Backups von Betriebssystemen sind auch sinnvoll, wenn nur ein paar Systemdateien wiederhergestellt werden müssen (z.B. durch unabsichtliches Löschen).

Applikations-Software

Diese Daten ändern sich, wenn Applikationen installiert, aktualisiert oder gelöscht werden.

Applikationsdaten

Diese Daten ändern sich so oft wie die jeweiligen Applikationen ausgeführt werden. Abhängig von der jeweiligen Applikation und Ihrem Unternehmen kann dies bedeuten, dass die Änderung jede Sekunde stattfindet oder einmal am Ende des Geschäftsjahres.

Benutzerdaten

Diese Daten ändern sich mit dem Verhaltensmuster der Benutzergemeinschaft. Für die meisten Unternehmen bedeutet dies, dass es ständig Änderungen gibt.

Basierend auf diesen Kategorien (und den zusätzlichen Kategorien, die speziell für Ihr Unternehmen zutreffen) sollten Sie jetzt zumindest gut über die Art von Backups Bescheid wissen, die Sie benötigen, um Ihre Daten zu sichern.

4. Der Begriff *Daten* in diesem Abschnitt beschreibt alles, das über Backup-Software verarbeitet wird. Dies umfasst Betriebssystemsoftware, Applikationssoftware sowie die eigentlichen Daten. Egal um welche Art Informationen es sich handelt, für Backup-Software sind dies alles Daten.

Anmerkung

Sie sollten beachten, dass die meiste Backup-Software mit Daten auf Verzeichnis- oder Dateisystemlevel umgeht. Mit anderen Worten spielt die Verzeichnisstruktur Ihres Systems eine Rolle bei der Art und Weise, wie Backups durchgeführt werden. Dies ist ein weiterer Grund, warum es immer eine gute Idee ist, die beste Verzeichnisstruktur für ein neues System sorgfältig zu planen und Dateien und Verzeichnisse in Bezug auf die jeweilige Verwendung zu gruppieren.

8.2.2. Backup-Software - Kaufen versus Erstellen

Um Backups durchzuführen, müssen Sie als erstes die richtige Software besitzen. Diese Software muss nicht nur in der Lage sein, Bits auf Backup-Medien zu kopieren, sondern auch mit den Personal- und Geschäftsbedürfnissen Ihres Unternehmens übereinstimmen. Einige Features, die Sie bei der Auswahl Ihrer Backup-Software in Betracht ziehen sollten, umfassen:

- Die Planung von Backups zu einem angemessenen Zeitpunkt
- Die Verwaltung des Ortes, der Rotation und der Verwendung von Backup-Medien
- Das Arbeiten mit Operatoren (und/oder automatischen Medienwechslern), um sicherzustellen, dass die richtigen Medien zur Verfügung stehen.
- Die Unterstützung von Operatoren im Auffinden der Medien, die ein bestimmtes Backup einer Datei enthalten

Wie Sie sehen, umfasst eine realistische Backup-Lösung wesentlich mehr als nur das Kritzeln von Bits auf Backup-Medien.

Die meisten Systemadministratoren betrachten zu diesem Zeitpunkt zwei Lösungen:

- Den Kauf einer kommerziell entwickelten Lösung
- Das Erstellen eines im Hause entwickelten Backup-Systems (mit einer möglichen Integration einer oder mehrerer Open Source Technologien)

Jeder Ansatz hat seine Vor- und Nachteile. Bedingt durch die Komplexität der Aufgabe ist es eher unwahrscheinlich, dass selbstentwickelte Software einige Aspekte (z.B. Medien-Management oder umfangreiche Dokumentation und technischen Support) sehr gut durchführen kann. Für einige Unternehmen ist dies jedoch eher irrelevant.

Eine kommerziell entwickelte Lösung ist wahrscheinlich funktionaler, kann aber auch viel zu komplex für die Ansprüche des Unternehmens sein. Auf der anderen Seite kann die Komplexität aber auch genutzt werden, um bei dieser Lösung zu bleiben, sollte das Unternehmen wachsen.

Wie Sie sehen gibt es keine eindeutige Methode für die Entscheidung für ein Backup-System. Die einzige Richtlinie, die wir Ihnen geben können, ist folgende Punkte zu betrachten:

- Das Ändern von Backup-Software ist schwierig. Einmal implementiert, werden Sie diese Software sehr lange verwenden; Sie haben schließlich Langzeit-Backup-Archive, die Sie lesen können müssen. Das Wechseln von Backup-Software bedeutet, dass Sie die ursprüngliche Software behalten müssen (um auf die Archive zugreifen zu können) oder Sie müssen die Backup-Archive konvertieren, so dass diese mit der neuen Software kompatibel sind.

  Abhängig von der Backup-Software sind die Anstrengungen, die in das Konvertieren von Backup-Archiven gesteckt werden müssen, relativ niedrig (jedoch zeitaufwendig), wie das Laufenlassen der Backups durch ein bereits bestehendes Konvertierungsprogramm oder erfordern ein reversives Engineering des Backup-Formats und das Erstellen benutzerdefinierter Software, um diese Aufgabe durchzuführen.

- Die Software muss 100% zuverlässig sein — sie muss genau das tun, was von ihr verlangt wird, wenn es von ihr verlangt wird.
- Wenn es nötig wird, jegliche Daten zu sichern — ob eine einzelne Datei oder ein komplettes Dateisystem — muss die Backup-Software 100% verlässlich sein.

8.2.3. Arten von Backups

Die allgemeine Meinung über Computer-Backups ist, dass diese eine identische Kopie *aller* Daten auf dem Computer darstellen. Anders gesagt, wenn ein Backup an einem Dienstag abend erstellt wurde, und sich den ganzen Mittwoch über nichts ändert, ist das Backup am Mittwoch identisch mit dem Backup vom Dienstag.

Auch wenn es möglich ist, Backups so zu konfigurieren, ist es eher unwahrscheinlich, das Sie dies tun. Um ein tieferes Verständnis zu erlangen, müssen wir erst die verschiedenen Arten von Backups betrachten. Diese sind:

- Vollständige Backups
- Inkrementelle Backups
- Differentielle Backups

8.2.3.1. Vollständige Backups

Die Art des Backups, die zu Beginn dieses Kapitels erwähnt wurde, ist als *vollständiges Backup* bekannt. Bei einem vollständigen Backup wird jede einzelne Datei auf das Backup-Medium geschrieben. Wie oben erwähnt, sind die Backups identisch, solange sich keine Daten ändern.

Diese Ähnlichkeit hängt von der Tatsache ab, dass ein vollständiges Backup nicht prüft, ob sich eine Datei seit dem letzten Backup geändert hat. Alle Daten werden blind auf das Backup-Medium geschrieben, ob diese geändert wurden oder nicht.

Vollständige Backups werden aus folgendem Grund nicht ständig durchgeführt — jede einzige Datei wird auf das Backup-Medium geschrieben. Dies bedeutet, dass ein Großteil des Backup-Mediums für immer die gleichen Daten verschwendet wird. Das abendliche Sichern von 100 Gigabytes, wenn sich nur 10 Megabytes geändert haben, scheint nicht der logischste Ansatz zu sein; deshalb wurden *Inkrementelle-Backups* geschaffen.

8.2.3.2. Inkrementelle-Backups

Im Gegensatz zu vollständigen Backups prüfen Inkrementelle Backups als erstes, ob das Änderungsdatum einer Datei neuer ist als das des letzten Backups. Ist dies nicht der Fall, wurde die Datei seit dem letzten Backup nicht geändert und wird nicht in das Backup aufgenommen. Ist jedoch das Änderungsdatum *neuer* als das letzte Backup-Datum, wurde die Datei geändert und sollte gesichert werden.

Inkrementelle Backups werden zusammen mit einem regelmäßigen, vollständigen Backup eingesetzt (z.B. ein vollständiges Backup jede Woche plus tägliche Inkrementelle-Backups).

Der Hauptvorteil der Inkrementelle Backups ist, dass diese schneller sind als vollständige Backups. Der Hauptnachteil ist, dass das Wiederherstellen einer Datei u.U. bedeutet, mehrere Inkrementelle Backups zu durchsuchen, bis die richtige Datei gefunden wurde. Bei der Wiederherstellung eines kompletten Dateisystems ist es notwendig, das letzte vollständige Backup wiederherzustellen und dann jedes darauffolgende Inkrementelle Backup.

Um das Durchsuchen jedes Inkrementellen Backups zu umgehen, wurde ein leicht unterschiedlicher Ansatz implementiert. Dieser ist als *Differentielles Backup* bekannt.

8.2.3.3. Differentielle Backups

Differentielle Backups ähneln Inkrementellen Backups, indem beide nur geänderte Dateien sichern. Differentielle Backups sind jedoch *kumulativ* — d.h. dass wenn eine Datei geändert wurde, diese in allen nachfolgenden Backups mitaufgenommen wird (bis zum nächsten vollständigen Backup).

Die bedeutet, dass jedes Differentielle Backup alle seit dem letzten vollständigen Backup geänderten Dateien enthält und somit eine vollständige Wiederherstellung mit dem letzten vollständigen Backup und dem letzten Differentiellen Backup möglich ist.

Wie die Backup-Strategie für Inkrementelle Backups folgen Differential Backups gewöhnlich dem gleichen Ansatz: ein einzelnes, regelmäßiges vollständiges Backup und häufigere Differentielle Backups.

Der Nachteil von Differentiellen Backups auf diese Weise ist, dass diese mit der Zeit ziemlich groß werden können (davon ausgehend, dass verschiedene Dateien zwischen den vollständigen Backups verändert werden). Dies platziert Differentielle Backups zwischen Inkrementelle Backups und vollständigen Backups in Bezug auf den Einsatz von Backup-Medien und Backup-Geschwindigkeit, wobei meistens schnellere Wiederherstellungen von einzelnen Dateien und vollständigen Systemen geboten werden (aufgrund weniger Backups, die durchsucht/wiederhergestellt werden müssen).

Durch diese Charakteristika sind Differentielle Backups auf jeden Fall eine Überlegung wert.

8.2.4. Backup-Medien

Wir haben den Begriff "Backup-Medien" in den vorherigen Abschnitten nur vorsichtig verwendet. Und hierfür gibt es einen Grund. Die meisten erfahrenen Systemadministratoren denken bei Backups sofort an das Lesen und Beschreiben von Bändern. Heutzutage gibt es jedoch weitere Optionen.

Eine zeitlang waren Bandgeräte die einzigen portablen Mediengeräte, die für Backup-Zwecke eingesetzt werden konnten. Dies hat sich jedoch geändert. In den folgenden Abschnitten betrachten wir die bekanntesten und beliebtesten Backup-Medien und bieten einen Überblick über deren Vorteile und Nachteile.

8.2.4.1. Band

Band war das erste, weitverbreitete portable Daten-Speichermedium. Es hat die Vorteile geringer Kosten und relativ guter Speicherkapazität. Band hat jedoch auch einige Nachteile — es ist Verschleißanfällig, und der Zugriff auf Daten erfolgt sequentiell.

Diese Faktoren bedeuten, dass man einen Überblick über die Bandnutzung behalten sollte (Bänder nach Ablauf ihrer Lebensdauer in den Ruhestand versetzen) und dass das Suchen nach einer bestimmten Datei auf Band zu einer langwierige Angelegenheit werden kann.

Auf der anderen Seite ist Bandspeicher das kostengünstigste Massenspeichermedium auf dem Markt und verfügt über erprobte Verlässlichkeit. Dies bedeutet, dass das Aufbauen einer vernünftig großen Band-Bibliothek nicht einen Großteil Ihres Budgets in Anspruch nimmt und Sie sich darauf verlassen können, diese jetzt und auch in Zukunft verwenden zu können.

8.2.4.2. Festplatte

Festplatten wurden bisher nicht als Backup-Medien in Betracht gezogen. In letzter Zeit sind jedoch die Preise für Speichermedien soweit gesunken, dass es sich in einigen Fällen auszahlt, Festplatten als Backup-Speicher einzusetzen.

Der Hauptgrund für den Einsatz von Festplatten als Speichermedium ist deren Geschwindigkeit. Es gibt bisher kein schnelleres Massenspeicher-Medium auf dem Markt. Geschwindigkeit kann zu einem

kritischen Faktor werden, wenn die Zeit zum Speichern von Daten relativ kurz ist und die Datenmengen groß sind.

Festplatten sind jedoch nicht das ideale Backup-Medium. Gründe sind unter anderem Folgende:

- Festplatten sind generell nicht portabel. Ein Schlüsselfaktor einer effektiven Backup-Strategie ist, die Backups extern zu lagern. Ein Backup Ihrer Produktionsdaten, das sich auf einer Festplatte einen Meter entfernt von der eigentlichen Datenbank befindet, ist kein Backup sondern eine Kopie. Und Kopien sind im Falle, das das Datencenter und alles darin (inklusive Ihrer Kopien) durch unglückliche Umstände beschädigt oder zerstört werden, nicht gerade hilfreich.
- Festplatten sind relativ kostenintensiv (zumindest verglichen mit anderen Backup-Medien). Es gibt Situationen, in denen Geld keine Rolle spielt, in allen anderen Situationen bedeutet dies jedoch, die Ausgaben für Festplatten als Backup-Speicher so gering wie möglich zu halten, indem die Anzahl der Backup-Kopien so gering wie möglich gehalten wird. Weniger Backup-Kopien bedeutet weniger Redundanz, sollte ein Backup aus irgendeinem Grund nicht lesbar sein.
- Festplatten sind zerbrechlich. Auch wenn Sie Geld in portable Festplatten investieren, kann die Zerbrechlichkeit zum Problem werden. Lassen Sie eine Festplatte fallen, verlieren Sie Ihr Backup. Es sind besondere Boxen erhältlich, die dieses Risiko reduzieren (jedoch nicht vollständig ausschalten), was das Ganze jedoch noch kostpieliger macht.
- Festplatten sind keine Archivmedien. Auch wenn Sie alle Probleme, die bei Backups auf Festplatten auftreten können, bewältigen, sollten Sie Folgendes beachten. Die meisten Unternehmen unterliegen diversen rechtlichen Bestimmungen für das Aufbewahren von Daten für einen bestimmten Zeitraum. Die Wahrscheinlichkeit, brauchbare Daten von einem 20-Jahre alten Band zu erhalten, ist wesentlich größer als die von einer 20-Jahre alten Festplatte. Haben Sie zum Beispiel die nötige Hardware, um diese mit Ihrem System zu verbinden? Ein weiteres Problem ist, dass eine Festplatte wesentlich komplexer ist als eine Bandkassette. Wenn ein 20-Jahre alter Motor einen 20-Jahre alten Bandteller antreibt, und somit 20-Jahre alte Lese/Schreibköpfe über diesen Teller fahren, wie groß ist die Chance, dass alle diese Komponenten nach 20 Jahren Stillstand noch problemlos funktionieren?

Anmerkung

Einige Datencenter führen Backups auf Festplatten durch und archivieren dann nach Beendigung der Backups diese auf Band. Dies ermöglicht die schnellsten Backups in einem kurzen Backup-Zeitrahmen. Das Speichern der Backups auf Band kann dann im Laufe des Arbeitstages geschehen; so lange das "Aufzeichnen" beendet ist, bevor das nächste Backup gemacht wird. Zeit spielt hier keine Rolle.

Auch nach all diesen Argumenten gibt es doch immer noch Situationen, in denen Backups auf Festplatten Sinn ergeben. Im nächsten Abschnitt betrachten wir, wie diese mit einem Netzwerk zusammen verwendet werden können, um eine praktikable (wenn auch teure) Backup-Lösung zu formen.

8.2.4.3. Netzwerk

Alleine kann ein Netzwerk nicht als Backup-Medium wirken. Zusammen mit Massenspeicher-Technologien funktioniert dies jedoch recht gut. Wenn Sie zum Beispiel ein Hochgeschwindigkeits-Netzwerk mit einem entfernten Datencenter verknüpfen, das sehr viel Speicherplatz bietet, sind die vorher erwähnten Nachteile des Backups auf Festplatten auf einmal keine Nachteile mehr.

Indem Sie die Backups über das Netzwerk durchführen, befinden sich die Festplatten bereits extern, d.h. der Transport zerbrechlicher Festplatten entfällt. Durch entsprechende Bandweite kann der Geschwindigkeitsvorteil von Festplatten aufrecht erhalten werden.

Dieser Ansatz löst jedoch nicht das Problem der Archivierung (es kann jedoch wie bereits erwähnt die "Backup auf Band archivieren"-Methode verwendet werden). Zusätzlich dazu lassen die Kosten eines entfernten Datencenters mit einer Hochgeschwindigkeitsverbindung zum Hauptdatencenter diese Lösung extrem teuer werden. Unternehmen, die diese Art von Features benötigen, sind jedoch sicherlich bereit, diese Kosten zu tragen.

8.2.5. Lagern von Backups

Was passiert nachdem die Backups vollständig sind? Die offensichtliche Antwort ist, dass diese irgendwo gelagert werden müssen. Was jedoch nicht so offensichtlich ist, ist was genau gelagert werden soll — und wo.

Um diese Fragen zu beantworten, müssen wir uns erst überlegen, unter welchen Umständen diese Backups verwendet werden sollen. Es gibt drei Hauptsituationen:

1. Geringfügige, spontane Anfragen von Benutzern
2. Umfassende Wiederherstellung nach einem Disaster
3. Archivierung mit geringster Wahrscheinlichkeit, jemals wieder verwendet zu werden

Leider gibt es unversöhnliche Widersprüche zwischen 1 und 2. Falls ein Benutzer eine Datei versehentlich löscht, möchte er diese sofort wiederhergestellt haben. Dies impliziert, dass das Backup-Medium nicht mehr als ein paar Schritte entfernt von dem System ist, auf dem die Daten wiederhergestellt werden sollen.

Im Falle eines Disasters, das eine vollständige Wiederherstellung einer oder mehrerer Computer in Ihrem Datencenter nötig macht und dieses Disaster physikalischer Natur war, so wurden mit der Zerstörung Ihrer Computer höchstwahrscheinlich auch die Backups zerstört, die sich nur ein paar Schritte entfernt befanden. Dies wäre ganz und gar nicht wünschenswert.

Archivierung ist weniger problematisch, da die Wahrscheinlichkeit, dass das Archiv jemals wieder für irgendeinen Zweck verwendet wird, relativ gering ist. Selbst wenn die Backup-Medien Kilometer vom Datencenter entfernt lagern, würde dies kein großes Problem darstellen.

Die Schritte, die zur Lösung Probleme eingeleitet werden, hängen von den Bedürfnissen des jeweiligen Unternehmens ab. Ein möglicher Ansatz ist, Backups der letzten paar Tage vor-Ort zu lagern und diese dann an einen sicheren externen Ort zu verlagern, sobald neue Backups vorliegen.

Ein anderer Ansatz ist, zwei verschiedene Medien-Pools zu halten:

- Einen Datencenter-Pool nur für spontane Wiederherstellungsanfragen
- Einen externen Pool für externe Lagerung und Wiederherstellung nach einem Disaster

Dies bedeutet jedoch, dass für zwei Pools auch jeweils zwei Backups angefertigt oder diese Backups kopiert werden müssen. Dies ist grundsätzlich möglich, kann jedoch zeitaufwendig sein. Das Kopieren benötigt auch mehrere Backup-Platten, um die Kopien zu verarbeiten (und zusätzlich ein System für das eigentliche Kopieren).

Die Herausforderung für den Systemadministrator ist es, einen Ausgleich zu schaffen, sodass alle Bedürfnisse in Betracht gezogen werden und Backups für den schlimmsten Fall zur Verfügung stehen.

8.2.6. Wiederherstellung

Während Backups täglich durchgeführt werden, sind Wiederherstellungen ein eher seltenes Vorkommnis. Wiederherstellungen sind jedoch unvermeidbar. Eines Tages werden diese notwendig sein und darauf sollten Sie sich vorbereiten.

Das Wichtigste ist, sich die verschiedenen Wiederherstellungsszenarien in diesem Abschnitt anzuschauen und Wege festzulegen, um Ihre Fähigkeiten diese auszuführen, zu testen. Und denken Sie daran, dass der schwerste auch immer der kritischste Weg ist.

8.2.6.1. Wiederherstellen von "Bare Metal"

Der Term "restoring from bare metal" ist die Umschreibung eines Systemadministrators für den Prozess der Datenwiederherstellung auf einem Computer, auf dem sich sonst überhaupt keine Daten befinden — kein Betriebssystem, keine Applikationen, nichts.

Es gibt zwei Ansätze für Bare-Metal-Restoration:

Neuinstallation, gefolgt von einer Wiederherstellung

Hierbei wird das Betriebssystem wie bei einem neuen Computer völlig neu installiert. Sobald das Betriebssystem funktioniert und richtig konfiguriert ist, können die übrigen Festplatten konfiguriert und formatiert werden und alle Backups von Backup-Medien wiederhergestellt werden.

Rettungsdisketten

Eine Rettungsdiskette ist ein bootbares Medium (meistens CD-ROM), das eine minimale Systemumgebung enthält und die meisten grundlegenden Systemverwaltungsaufgaben bewältigen kann. Die Umgebung der Rettungsdiskette enthält die nötigen Utilities für das Partitionieren und Formatieren von Festplatten, die nötigen Gerätetreiber zum Zugriff auf das Backup-Gerät und die nötige Software, um Daten vom Backup-Medium wiederherzustellen.

Anmerkung

Einige Computer haben die Fähigkeit, bootbare Backup-Bänder zu erstellen, und von diesen zu booten, um den Wiederherstellungsprozess zu starten. Diese Fähigkeit besitzen jedoch nicht alle Computer. Generell können insbesondere Computer dies nicht, die auf der PC-Architektur basieren.

8.2.6.2. Testen von Backups

Jedes Backup sollte in regelmäßigen Abständen getestet werden, um sicherzustellen, dass Daten auch gelesen werden können. Tatsache ist, dass manche Backups aus irgendeinem Grund manchmal nicht lesbar sind. Das Schlimme daran ist, dass dies häufig nicht rechtzeitig bemerkt wird, sondern erst dann, wenn alle Daten verloren sind und vom Backup wiederhergestellt werden müssen.

Die Gründe hierfür reichen von Änderungen in der Bandkopf-Ausrichtung über Fehlkonfigurationen in der Backupssoftware bis hin zu Bedienungsfehlern. Der Grund ist jedoch relativ unwichtig, denn ohne regelmäßiges Testen können Sie nicht sicher sein, dass Sie Backups erstellen, von denen Daten zu einem späteren Zeitpunkt wiederhergestellt werden können.

8.3. Wiederherstellung nach einem Disaster

Machen Sie beim nächsten Mal, wenn Sie Ihr Datencenter betreten, ein kleines Gedankenexperiment: stellen Sie sich vor, das Datencenter ist nicht mehr da. Und dies betrifft nicht nur die Computer. Das gesamte Gebäude ist weg. Stellen Sie sich jetzt vor, Ihr Job ist es, die gesamte Arbeit, die in diesem Datencenter vollbracht wurde, irgendwie wiederherzustellen, egal wie, egal wo, so schnell wie möglich. Was würden Sie tun?

Indem Sie darüber ernsthaft nachdenken, haben Sie den ersten Schritt zur Wiederherstellung nach einer Katastrophe getan. Wiederherstellung ist die Fähigkeit, sich von einem Ereignis, das die Funktion Ihres Datencenters erheblich beeinträchtigt hat, so schnell und vollständig wie möglich zu erholen. Die Art der Katastrophe ist unterschiedlich, aber das Endziel ist immer das gleiche.

Die Schritte für die Wiederherstellung nach einer Katastrophe sind vielzählig und breit gefächert. Im Folgenden erhalten Sie einen hochrangigen Überblick über den Prozess zusammen mit einigen Schlüsselfaktoren, die Sie im Auge behalten sollten.

8.3.1. Erstellen, Testen und Implementieren eines Wiederherstellungsplans nach Katastrophen

Ein Backup-Ort ist lebenswichtig, aber völlig nutzlos ohne einen Wiederherstellungsplan. Dieser Plan gibt jeden Aspekt des Wiederherstellungsplans einschließlich - jedoch nicht ausschließlich - Folgendem vor:

- Welche Ereignisse einer Katastrophe vorausgehen
- Welche Mitarbeiter im Unternehmen befugt sind, den Katastrophenstand auszurufen und somit den Plan ins Leben zu rufen
- Die Abfolge der Ereignisse, die nötig sind, um den Backup-Ort vorzubereiten, wenn eine Katastrophe ausgerufen wurde
- Die Rollen und Verantwortlichkeiten aller Beteiligten in Bezug auf das Ausführen des Plans
- Eine Bestandsaufnahme der benötigten Hardware und Software, um die Produktion wiederherzustellen
- Ein Plan, auf dem alle Mitarbeiter aufgeführt sind, die den Backup-Ort besetzen, inklusive Rotationsplan, um den laufenden Betrieb zu unterstützen, ohne das Katastrohenschutzteam völlig zu überanspruchen.
- Die Abfolge der Ereignisse, die nötig sind, um den Betrieb vom Backup-Ort zurück in das restaurierte/neue Datencenter zurückzuverlagern

Diese Pläne füllen oftmals mehrere Aktenordner. Diese Detailfülle ist wichtig, da dieser Plan vielleicht das Letzte ist, was von Ihrem alten Datencenter übrig ist (von den extern-gelagerten Backups abgesehen), um Ihnen bei der Wiederherstellung des Betriebs zu helfen.

Tipp

Während Wiederherstellungspläne direkt an Ihrem Arbeitsplatz zur Verfügung stehen sollten, ist es jedoch sinnvoll, Kopien extern zu lagern. Auf diese Weise wird durch eine Katastrophe nicht jede Kopie des Plans zerstört. Eine gute Lagerstätte ist das externe Backup-Lager. Werden keine Sicherheitsrichtlinien Ihres Unternehmens verletzt, ist ein weiterer guter Lagerplatz das Haus eines Mitarbeiters.

Solch ein wichtiges Dokument verdient ernsthafte Überlegungen (und evtl. professionelle Hilfe bei der Erstellung).

Sobald dieses Dokument erstellt ist, muss das Wissen darin regelmäßig getestet werden. Das Testen eines Wiederherstellungsplans umfasst das eigentliche Durchführen aller Schritte: Das Einrichten eines temporären Datencenters am externen Backup-Ort, das Ausführen von Applikationen und das Fortfahren des normalen Betriebs wenn das "Disaster" vorbei ist. Die meisten Tests versuchen nicht, 100% aller Aufgaben im Plan zu erreichen; anstelle dessen wird ein repräsentatives System und eine Applikation ausgewählt, die dann ins Lager verlegt, in Produktion genommen und am Ende des Tests zum normalen Betrieb zurückgeführt werden.

Anmerkung

Auch wenn dies leicht abgedroschen klingt, muss der Plan ein lebendiges Dokument sein. Wenn sich die Daten ändern, muss sich dies im Plan wiederspiegeln. Auf viele Arten ist ein veralteter Disasterplan schlimmer als gar keiner. Nehmen Sie sich also Zeit und führen Sie regelmäßige (z.B. alle Vierteljahre) eine Durchsicht und Aktualisierungen durch.

8.3.2. Backup-Orte: Kalt, Warm und Heiß

Eines der wichtigsten Aspekte der Wiederherstellung ist der Ort, von dem aus die Wiederherstellung durchgeführt werden kann. Dieser Ort ist bekannt als *Backup-Ort* Im Falle eines Disasters wird an diesem Ort dasDatencenter erschaffen, von dem aus der Betrieb für die Dauer der Katastrophe weitergeführt wird.

Es gibt drei Arten von Backup-Orten:

- Kalte
- Warme
- Heiße

Offensichtlich beziehen sich diese Begriffe nicht auf die Temperatur des Ortes. Sie beziehen sich auf den Aufwand, der aufgebracht werden muss, um den Betrieb am Backup-Ort im Falle einer Katastrophe aufzunehmen.

Ein kalter Ort ist wenig mehr als ein angemessen konfigurierter Raum in einem Gebäude. Alles nötige zur Wiederherstellung des Services für die Benutzer muss beschafft und hierher geliefert werden, bevor die Wiederherstellung beginnen kann. Wie Sie sich vorstellen können, geht dies mit einer erheblichen Verzögerung von einem kalten Ort bis hin zum voll-funktionsfähigen Betrieb einher.

Kalte Orte sind die kostengünstigsten.

Ein warmer Backup-Ort ist bereit mit Hardware als angemessenes Abbild derer in Ihrem Datencenter ausgerüstet. Um den Service wiederherzustellen, müssen die neuesten Backups von der externen Lagerstätte geliefert und eine Bare-Metal-Wiederherstellung durchgeführt werden, bevor die eigentliche Wiederherstellungsarbeit beginnen kann.

Heiße Backup-Orte sind ein Abbild Ihres bisherigen Datencenters. Alle Systeme sind bereits konfiguriert und warten nur noch auf das neueste Backup von der externen Lagerstätte. Wie Sie sich vorstellen können, kann ein heißer Ort innerhalb von wenigen Stunden in Vollbetrieb versetzt werden.

Ein heißer Backup-Ort ist der teuerste von allen.

Backup-Orte können aus drei verschiedenen Quellen stammen:

- Unternehmen, die sich auf das Bereitsstellen von Wiederherstellungen nach einer Katastrophe spezialisieren
- Andere Orte, die Ihrem Unternehmen gehören und von diesem auch betrieben werden
- Eine Vereinbarung zwischen Ihnen und einem anderen Unternehmen, Datencenter-Einrichtungen im Falle einer Katastrophe gemeinsam zu verwenden.

Jeder Ansatz hat seine guten und schlechten Seiten. So hat das Verwenden einer Katastrophenschutz-Firma den Vorteil, dass Sie Zugang zu Experten haben, die Ihnen bei der Erstellung, Prüfung und Implementierung eines Planes helfen können. Dies ist jedoch leider nicht kostenlos.

Das Verwenden eines anderen Gebäudes, das Ihrem Unternehmen gehört, ist im allgemeinen eine Option zum Nulltarif. Das Ausrüsten und Warten ist jedoch relativ kostenintensiv.

Eine Vereinbarung über das Teilen eines Datencenters mit einem anderen Unternehmen kann sehr günstig sein. Jedoch ist ein langfristiger Betrieb unter solchen Bedingungen meistens nicht möglich, da das Datencenter des Gastgebers den normalen Betrieb aufrechterhalten muss und somit die Situation bestenfalls angespannt ist.

Am Ende ist die Auswahl eines Backup-Ortes ein Kompromiss zwischen Kosten und dem Bedarf der Firma, die Produktion aufrecht zu erhalten.

8.3.3. Hardware- und Softwareverfügbarkeit

Ihr Wiederherstellungplan muss Methoden für die Beschaffung der nötigen Hardware und Software für den Betrieb am Backup-Ort beinhalten. Ein professionell verwalteter Backup-Ort kann u.U. schon alles haben, was Sie brauchen (oder Sie müssen evtl die Beschaffung und Lieferung spezieller Materialien organisieren). Auf der anderen Seite bedeutet ein kalter Ort, dass eine verlässliche Quelle für jede einzelne Komponente gefunden werden muss. Meistens arbeiten Unternehmen mit Herstellern zusammen, um Vereinbarungen über Lieferungen von Hardware und/oder Software im Katastrophenfall zu treffen.

8.3.4. Backup-Verfügbarkeit

Wird der Katastrophenstand ausgerufen, müssen Sie Ihre externe Lagerstätte aus folgenden Gründen benachrichtigen:

- Um die neuesten Backups zum Backup-Ort zu liefern
- Um ein regelmäßiges Abholen und Anliefern von Backups für den Backup-Ort (zusätzlich zu den normalen Backups) zu arrangieren.

Tipp

Im Falle einer Katastrophe sind die letzten Backups, die Sie von Ihren alten Daten haben, von essentieller Bedeutung. Überlegen Sie, ob Sie Kopien anfertigen sollten, bevor irgendetwas anderes gemacht wird, um die Originale so schnell wie möglich wieder ins Lager zu schaffen.

8.3.5. Netzwerverbindung zum Backup-Ort

Ein Datencenter ist nicht wirklich nützlich, wenn es vollständig getrennt vom Rest des Unternehmens ist. Abhängig vom Katastrophenplan und der Art der Katastrophe befindet sich die Benutzergemeinschaft evtl. kilometerweit entfernt vom Backup-Ort. In diesem Fall ist eine Verbindung für die Wiederherstellung des Betriebs bedeutend.

Eine andere Verbindung, die Sie im Hinterkopf behalten sollten, ist das Telefon. Sie müssen sicherstellen, dass genügend Telefonleitungen für jegliche verbale Kommunikation mit den Benutzern zur Verfügung steht. Was mal ein einfacher Ruf durch das Büro war, wird jetzt zu einem Ferngespräch. Planen Sie deshalb zusätzlich Telefonverbindungen ein, die anfangs nicht notwendig erschienen.

8.3.6. Belegschaft des Backup-Ortes

Das Problem der Mitarbeiter-Belegung ist vielschichtig. Ein Aspekt des Problems ist die Entscheidung, wieviele Mitarbeiter im Backup-Datencenter benötigt werden. Während eine Notbelegschaft

den Betrieb für eine kurze Zeit aufrecht erhalten kann, wird, falls die Katastrophe andauert, mehr Personal benötigt, um unter diesen außergewöhnlichen Umständen den Betrieb zu gewährleisten.

Dies umfasst, dass das Personal genügend Zeit hat, sich zu erholen und unter Umständen dazu an deren Wohnort zurückzureisen kann. War die Katastrophe weitreichend genug, um Heim und Familie Ihrer Mitarbeiter zu betreffen, muss außerdem zusätzlich Zeit für persönliche Wiederherstellung gegeben werden. Temporäre Unterkünfte in der Nähe des Backup-Ortes sind nötig, zusammen mit Transport, um die Mitarbeiter vom Backup-Ort zu deren Unterkünften zu transportieren.

Häufig enthält ein Katastrophen-Plan vor-Ort Mitarbeiter als Repräsentanten der Benutzergemeinschaft des Unternehmens. Dies hängt von der Fähigkeit Ihres Unternehmens ab, mit einem entfernten Datencenter zu arbeiten. Müssen diese Repräsentanten am Backup-Ort arbeiten. müssen ähnliche Provisionen für diese geschaffen werden.

8.3.7. Rückkehr zum Normalzustand

Irgendwann hat jede Katastrophe ein Ende. Der Plan muss diese Phase auch beihalten. Das neue Datencenter muss mit all der nötigen Hardware- und Software ausgerüstet sein. Während diese Phase nicht die zeitkritische Natur der Vorbereitungen hat, die gemacht wurden, als die Katastrophe bekannt wurde, kosten Backup-Orte jedoch jeden Tag Geld. Aus ökonomischen Gründen muss also der Übergang so schnell als möglich von statten gehen.

Es müssen die letzten Backups vom Backup-Ort durchgeführt und an das neue Datencenter geliefert werden. Nachdem die Daten auf der neuen Hardware wiederhergestellt wurden, kann die Produktion zum neuen Datencenter geschaltet werden.

Zu diesem Zeitpunkt kann das Backup-Datencenter außer Betrieb genommen werden. Dies umfasst auch jegliche temporäre Hardware, wie durch die letzten Abschnitte des Plans festgelegt. Zum Schluss wird die Effektivität des Plans überprüft und alle vorgeschlagenen Änderungen in einer aktualisierten Version des Plans integriert.

8.4. Red Hat Enterprise Linux-spezifische Informationen

Es gibt wenig im allgemeinen Kapitel über Disaster und Wiederherstellung, das einen direkten Einfluss auf ein bestimmtes Betriebssystem hat. Die Computer in einem überfluteten Datencenter wären so oder so betriebsunfähig, ob auf ihnen nun Red Hat Enterprise Linux oder ein anderes Betriebssystem läuft. Es gibt jedoch Teile von Red Hat Enterprise Linux, die sich auf bestimmte Aspekte der Wiederherstellung beziehen. Diese werden im folgenden Abschnitt beschrieben.

8.4.1. Software-Support

Als Softwarehersteller hat Red Hat eine Reihe von Support-Angeboten für seine Produkte, inklusive Red Hat Enterprise Linux. Mit diesem Handbuch halten Sie das allereinfachste Supporttool in den Händen. Dokumentation für Red Hat Enterprise Linux erhalten Sie auf der Red Hat Enterprise Linux Dokumentations-CD (die auf Ihrem Red Hat Enterprise Linux-System für schnellen Zugriff installiert werden kann), gedruckt in den verschiedenen Red Hat Enterprise Linux-Packungen und in elektronischer Form unter http://www.redhat.com/docs/.

Selbsthilfe-Optionen finden Sie in den vielen Mailinglisten von Red Hat (unter https://listman.redhat.com/mailman/listinfo/). Diese Mailinglisten machen Gebrauch vom gemeinschaftlichen Wissen der Red Hat-Benutzer-Gemeinschaft und zusätzlich dazu werden viele Listen von Red Hat-Mitarbeitern mitgelesen, die auch ihren Beitrag dazu leisten, wenn die Zeit es erlaubt. Desweiteren gibt es eine Wissensdatenbank auf der Red Hat-Webseite. Diese finden Sie auf der Hauptsupportseite von Red Hat unter http://www.redhat.com/apps/support/.

Es gibt noch weitere umfangreiche Support-Optionen. Informationen hierzu finden Sie auf der Red Hat-Webseite.

8.4.2. Backup-Technologien

Red Hat Enterprise Linux wird mit verschiedenen Programmen für das Durchführen von Backups und Wiederherstellen von Daten ausgeliefert. Jeweils für sich sind diese Dienstprogramme jedoch keine vollständige Backup-Lösung. Sie können jedoch als Kern für eine solche Lösung verwendet werden.

Anmerkung

Wie in Abschnitt 8.2.6.1 beschrieben, besitzen die meisten Computer, die auf einer Standard-PC-Architektur basieren, nicht die nötige Funktionalität, direkt von einem Backup-Band zu booten. Daraus folgend ist Red Hat Enterprise Linux nicht in der Lage, ein Booten vom Band auf solcher Hardware durchzuführen.

Sie können jedoch auch Ihre Red Hat Enterprise Linux CD-ROM als Rettungsdiskette verwenden. Weitere Informationen finden Sie im Kapitel über den Rettungsmodus im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

8.4.2.1. `tar`

Die `tar`-Utility ist unter UNIX-Systemadministratoren sehr bekannt. Es ist eine beliebte Archivierungsmethode für das gemeinsame Verwenden von Source Code und Dateien auf mehreren Systemen. Die `tar` Implementierung in Red Hat Enterprise Linux ist GNU `tar`, eine der `tar`-Implementierungen, die mehr Features besitzt.

Mithilfe von `tar` ist das Sichern von Inhalten eines Verzeichnisses so einfach wie das Eingeben des folgenden Befehls:

```
tar cf /mnt/backup/home-backup.tar /home/
```

Dieser Befehl erstellt ein Archiv mit dem Namen `home-backup.tar` in `/mnt/backup/`. Das Archiv enthält den Inhalt des `/home/` Verzeichnisses.

Die resultierende Archivdatei ist fast so groß wie die zu sichernden Datenmengen. Abhängig von der Art der Daten, die gesichert werden sollen, kann das Komprimieren der Archivdatei die Größe erheblich reduzieren. Die Archivdatei kann durch das Hinzufügen einer einzigen Option zur vorherigen Zeile komprimiert werden.

```
tar czf /mnt/backup/home-backup.tar.gz /home/
```

Die resultierende Archivdatei `home-backup.tar.gz` wird nun mit `gzip` komprimiert[5].

Es gibt viele Optionen für `tar`; weitere Informationen finden Sie auf der `tar(1)` man-Seite.

5. Die Erweiterung `.gz` wird traditionell verwendet, um anzuzeigen, dass die Datei mit `gzip` komprimiert wurde. Manchmal wird `.tar.gz` zu `.tgz` abgekürzt, um Dateinamen nicht zu lang werden zu lassen.

8.4.2.2. cpio

Die cpio-Utility ist ein anderes traditionelles UNIX-Programm. Es ist ein hervorragendes, allgemeines Programm für das Verschieben von Daten von einem Ort zum nächsten und dient so als gutes Backup-Programm.

Das Verhalten von cpio unterscheidet sich leicht von tar. Im Gegensatz zu tar liest cpio die Namen der Dateien, die verarbeitet werden sollen, über Standard-Eingabe. Eine allgemeine Methode, eine Liste von Dateien für cpio zu generieren, ist mit einem Programm wie find, dessen Ausgabe dann zu cpio geleitet wird:

```
find /home/ | cpio -o > /mnt/backup/home-backup.cpio
```

Dieser Befehl erstellt eine cpio-Archivdatei (die alles im /home/-Verzeichnis befindliche enthält) mit dem Namen home-backup.cpio, die im Verzeichnis /mnt/backup abgelegt wird.

Tipp

Dadurch dass find eine große Anzahl von Dateiauswahlprüfungen besitzt, können ausgereifte Backups erstellt werden. So führt zum Beispiel der folgende Befehl ein Backup nur der Dateien aus, die im letzten Jahr nicht geändert wurden:

```
find /home/ -atime +365 | cpio -o > /mnt/backup/home-backup.cpio
```

Es gibt noch viele andere Optionen für cpio (und find); weitere Informationen finden Sie auf den man-Seiten zu cpio(1) und find(1).

8.4.2.3. dump/restore: Nicht empfohlen für gemountete Dateisysteme!

Die Programme dump und restore sind die Linux-Äquivalente zu den gleichnamigen UNIX-Programmen. Als solche denken viele Systemadministratoren mit UNIX-Erfahrung, dass dump und restore gute Kandidaten für ein Backup-Programm unter Red Hat Enterprise Linux sind. Das Design des Linux-Kernels hat sich jedoch im Gegensatz zum dump-Design weiterentwickelt. Hier die Kommentare von Linus Torvalds zu diesem Thema:

```
From:  Linus Torvalds
To:  Neil Conway
Subject: Re: [PATCH] SMP race in ext2 - metadata corruption.
Date:  Fri, 27 Apr 2001 09:59:46 -0700 (PDT)
Cc:  Kernel Mailing List <linux-kernel At vger Dot kernel Dot org>

[ linux-kernel added back as a cc ]

On Fri, 27 Apr 2001, Neil Conway wrote:
> > I'm surprised that dump is deprecated (by you at least ;-)).  What to
> use instead for backups on machines that can't umount disks regularly?


Note that dump simply won't work reliably at all even in 2.4.x: the buffer
cache and the page cache (where all the actual data is) are not
coherent. This is only going to get even worse in 2.5.x, when the
directories are moved into the page cache as well.

So anybody who depends on "dump" getting backups right is already playing
Russian roulette with their backups.  It's not at all guaranteed to get the
right results - you may end up having stale data in the buffer cache that
```

```
ends up being "backed up".

Dump was a stupid program in the first place. Leave it behind.

> I've always thought "tar" was a bit undesirable (updates atimes or
> ctimes for example).

Right now, the cpio/tar/xxx solutions are definitely the best ones, and
will work on multiple filesystems (another limitation of "dump"). Whatever
problems they have, they are still better than the _guaranteed_(*)  data
corruptions of "dump".

However, it may be that in the long run it would be advantageous to have a
"filesystem maintenance interface" for doing things like backups and
defragmentation..

  Linus

(*) Dump may work fine for you a thousand times. But it _will_ fail under
the right circumstances. And there is nothing you can do about it.
```

Angesichts dieses Problems wird von der Benutzung von `dump`/`restore` auf gemounteten Dateisystemen strengstens abgeraten. Da `dump` jedoch ursprünglich dazu entwickelt worden war, um ungemountete Dateisysteme zu sichern, bleibt `dump` in Situationen, in denen ein Dateisystem auch offline mittels `umount` gebracht werden kann, aus diesem Grund nach wie vor eine funktionsfähige Backup-Methode.

8.4.2.4. Advanced Maryland Automatic Network Disk Archiver (AMANDA)

AMANDA ist eine Client/Server-basierte Backup-Applikation, die von der Universität Maryland, USA, erstellt wurde. Durch eine Client/Server-Architektur kann ein einziger Backup-Server (gewöhnlich ein leistungsstarkes System mit sehr viel freiem Platz auf schnellen Festplatten und mit der gewünschten Backup-Software konfiguriert) viele Client-Systemen sichern, auf denen nichts weiter als die AMANDA-Client-Software laufen muss.

Dieser Ansatz ist sehr sinnvoll, da die für Backups benötigten Ressourcen in einem System zusammengefasst werden, anstelle dass zusätzliche Hardware für jedes System, das Backup-Services benötigt, gebraucht wird. AMANDAs Design dient auch dazu, die Verwaltung von Backups zu zentralisieren und erleichtert somit das Leben des Systemadministrators.

Der AMANDA-Server verwaltet einen Pool von Backup-Medien und rotiert die Verwendung im Pool, sodass alle Backups für die vom Administrator vorgegebene Aufbewahrungszeit aufbewahrt werden. Alle Medien werden vorformatiert, so dass AMANDA erkennen kann, ob das richtige Medium zur Verfügung steht oder nicht. Zusätzlich dazu kann AMANDA mit automatischen Medien-Wechsel-Einheiten gekoppelt werden und ermöglicht so das vollständige Automatisieren der Backups.

AMANDA verwendet entweder `tar` oder `dump` für das Durchführen der eigentlichen Backups (unter Red Hat Enterprise Linux ist `tar` aufgrund der Probleme mit `dump`, wie in Abschnitt 8.4.2.3 beschrieben, vorzuziehen). Als solches benötigen AMANDA-Backups kein AMANDA zum Wiederherstellen von Dateien — ein eindeutiger Pluspunkt.

AMANDA wird normalerweise einmal am Tag während des Backupszeitraums des Datencenters ausgeführt. Der AMANDA-Server verbindet sich mit dem Client-System und weist diesen an, geschätzte Größen der durchzuführenden Backups herzustellen. Sobald alle diese Schätzungen zur Verfügung stehen, erstellt der Server einen Plan, indem automatisch festgelegt ist, in welcher Reihenfolge die Systeme gesichert werden.

Ist das Backup gestartet, werden die Daten über das Netzwerk vom Client zum Server gesendet, wo sie dann auf einer Festplatte gespeichert werden. Ist ein Backup vollständig, beginnt der Server, die Daten von der Festplatte auf ein Backup-Medium zu schreiben. Zum gleichen Zeitpunkt schicken

andere Clients ihre Backups zum Server zum Speichern auf der Festplatte. Dies resultiert in einem kontinuierlichen Datenstrom, der für das Schreiben auf das Backup-Medium zur Verfügung steht. Mit dem Schreiben der Backups auf das Backup-Medium werden diese vom Server gelöscht.

Sobald alle Backups abgeschlossen sind, erhält der Systemadministrator eine E-Mail mit dem Bericht über den Status der Backups, was ein Review schnell und einfach werden lässt.

Müssen Daten wiederhergestellt werden, enthält AMANDA ein Utility, mit dem das Dateisystem, Datum und Dateiname identifiziert werden können. Sobald dies geschehen ist, identifiziert AMANDA das richtige Backup-Medium, sucht die Daten und stellt diese wieder her. Wie bereits erwähnt, ermöglicht AMANDAs Design das Wiederherstellen von Daten auch ohne die Hilfe von AMANDA, auch wenn die Identifizierung der richtigen Medien dann ein langsamerer, manueller Vorgang wäre.

Dieser Abschnitt streift lediglich die einfachsten AMANDA-Konzepte. Weitere Informationen über AMANDA finden Sie auf der `amanda(8)` man-Seite.

8.5. Zusätzliche Ressourcen

In diesem Abschnitt werden verschiedene Ressourcen, die weiterführende Informationen zu Wiederherstellung nach Katastrophen und zu Red Hat Enterprise Linux-spezifischen Themen in diesem Kapitel bieten.

8.5.1. Installierte Dokumentation

Die folgenden Ressourcen sind auf einer typischen Red Hat Enterprise Linux-Installation enthalten und geben Ihnen weitere Informationen zu den in diesem Kapitel beschriebenen Themen.

- `tar(1)` man-Seite — Lernen Sie Daten zu archivieren.
- `dump(8))` man-Seite — Lernen Sie Dateisystem-Inhalte zu dumpen.
- `restore(8)` man-Seite — Lernen Sie wie Dateisystem-Inhalte, die durch `dump` gerettet worden sind, wiederhergestellt werden.
- `cpio(1)` man-Seite — Lernen Sie Dateien von und zu Archiven zu kopieren.
- `find(1)` man-Seite — Lernen Sie nach Dateien zu suchen.
- `amanda(8)` man-Seite — Lernen Sie mehr über die Befehle, die Teil des AMANDA-Backup-Systems sind.
- Dateien im `/usr/share/doc/amanda-server-<version>/` — Lernen Sie mehr über AMANDA, indem Sie diese unterschiedlichen Dokumente und Beispieldateien durchgehen.

8.5.2. Nützliche Webseiten

- http://www.redhat.com/apps/support/ — Die Red Hat Support-Homepage bietet leichten Zugriff auf verschiedene Ressourcen in Hinblick auf den Support von Red Hat Enterprise Linux.
- http://www.disasterplan.com/ — Eine interessante Seite mit Links zu vielen Seiten zur Wiederherstellung nach Katastrophen. Enthält einen Beispiel-Plan für den Katastrophenfall.
- http://web.mit.edu/security/www/isorecov.htm — Die Homepage des Massachusetts Institute of Technology Information Systems Business Continuity Planning enthält mehrere informative Links.
- http://www.linux-backup.net/ — Ein interessanter Überblick über die vielen Backup-bezogenen Angelegenheiten.

- http://www.linux-mag.com/1999-07/guru_01.html — Ein guter Artikel aus dem Linux Magazine über die eher technischen Aspekte der Durchführung von Backups unter Linux.
- http://www.amanda.org/ — Die Homepage des Advanced Maryland Automatic Network Disk Archiver (AMANDA).Enthält Referenzen zu verschiedenen AMANDA-Mailinglisten und anderen Online-Ressourcen.

8.5.3. Bücher zum Thema

Die folgenden Bücher behandeln verschiedene Themen der Wiederherstellung nach Katastrophen und sind eine gute Ressource für Red Hat Enterprise Linux-Systemadministratoren.

- Das *Red Hat Enterprise Linux Handbuch zur System-Administration*; Red Hat, Inc. — Enthält ein Kapitel zum Rettungsmodus, das sinnvoll für Bare-Metal-Wiederherstellungen ist.
- *Unix Backup & Recovery* von W. Curtis Preston; O'Reilly & Associates — Obwohl nicht direkt für Linux-Systemen geschrieben, enthält dieses Buch tiefgehende Informationen zu Backups und enthält sogar ein Kapitel zur Wiederherstellung nach Katastrophen.

Stichwortverzeichnis

Symbole

/etc/cups/, 156
/etc/fstab-Datei
  Aktualisieren, 114
  Dateisysteme mounten mit, 111
/etc/group-Datei
  Benutzer-Account, Rolle in, 143
  Gruppe, Rolle in, 143
/etc/gshadow-Datei
  Benutzer-Account, Rolle in, 144
  Gruppe, Rolle in, 144
/etc/mtab-Datei, 108
/etc/passwd-Datei
  Benutzer-Account, Rolle in, 141
  Gruppe, Rolle in, 141
/etc/printcap, 156
/etc/shadow-Datei
  Benutzer-Account, Rolle in, 142
  Gruppe, Rolle in, 142
/proc/mdstat-Datei, 121
/proc/mounts-Datei, 109
Änderungsüberwachung, 176
Überwachung
  Ressourcen, 15
  Systemleistung, 16
Überwachungsstatistiken
  Auswahl von, 16
  bandweiten-bezogen, 18
  CPU-bezogen, 17
  Speicher-bezogen, 19, 19

A

Abonnement-Registrierung, v
Account
  (Siehe Benutzer-Account)
Aktivieren Ihres Abonnements, v
Anschlagdrucker, 151
  Punktmatrix, 151
  Typenrad, 151
  Verbrauchsmaterialien, 152
  Zeile, 151
ATA Festplatte
  hinzufügen, 97
Ausführungsberechtigung, 139
Automatisierung, 9
  Überblick über , 1

B

Backups
  AMANDA Backup-Software, 192
  Arten von, 181
    Differentielle Backups, 182
    Inkrementelle Backups, 181
    Vollständige Backups, 181
  datenbezogene Angelegenheiten, 179
  Einführung in, 178
  Lagerung von, 184
  Medientypen, 182
    Band, 182
    Festplatte, 182
    Netzwerk, 183
  Planung, ändern, 101
  Software erstellen, 180
  Software kaufen, 180
  verwendete Technologien, 190
    cpio, 191
    dump, 191
    tar, 190
  Wiederherstellung, 184
    Bare-Metal-Wiederherstellung, 185
    Wiederherstellung testen, 185
Bandbreiten-bezogene Ressourcen
  (Siehe Ressorcen, System, Bandbreite)
Bash Shell, Automatisierung und, 9
Benutzer
  Wichtigkeit von, 6
Benutzer-Account
  Benutzername, 125
    Kollisionen in der Namensgebung, 126
    Namenskonventionen, 125
    Änderungen bei, 127
  Berechtigungen bezogen auf, 139
    ausführen, 139
    lesen, 139
    schreiben, 139
    Setgid, 139
    Setuid, 139
    Sticky Bit, 139
  Dateien, die kontrollieren, 141
    /etc/group, 143
    /etc/gshadow, 144
    /etc/passwd, 141
    /etc/shadow, 142
  GID, 140
  Heimverzeichnis
    zentralisiert, 138
  Passwort, 128
    die Kürze von, 129
    Erinnerungswert, 132
    Fälligkeit, 133
    geschrieben, 131
    großer Zeichensatz benutzt in, 132

kleiner Zeichensatz benutzt in, 130
länger, 132
mehrmals benutzt, 131
Personliche Information benutzt in, 131
schwach, 129
stark, 132
Wortspiele benutzt in, 131
Wörter benutzt in, 130
Ressourcen, deren Verwaltung, 136
System-GIDs, 140
System-UIDs, 140
Tools zum Verwalten, 144
chage-Befehl, 144
chfn-Befehl, 144
chpasswd-Befehl, 144
passwd-Befehl, 144
useradd-Befehl, 144
userdel-Befehl, 144
usermod-Befehl, 144
UID, 140
Verwaltung von, 125, 125, 134
Berufswechsel, 135
Kündigungen, 134
Neuzugänge, 134
Zugang zu gemeinsam genutzten Daten, 136
Zugriffskontrolle , 133
Benutzer-ID
(Siehe UID)
Benutzername, 125
Kollisionen zwischen, 126
Namenskonventionen, 125
ändern, 127
Berechtigungen, 139
Tools zum Verwalten
chgrp-Befehl, 146
chmod-Befehl, 146
chown-Befehl, 146

C

Cache-Speicher, 52
CD-ROM
Dateisystem
(Siehe ISO 9660-Dateisystem)
chage-Befehl, 144
chfn-Befehl, 144
chgrp-Befehl, 146
chmod-Befehl, 146
chown-Befehl, 146
chpasswd-Befehl, 144
CPU-Leistung
(Siehe Ressourcen, System, Prozessleistung)
CUPS, 156

D

Das Unerwartete, Vorbereitung für, 8
Dateinamen
Gerät, 103
Dateisystem
Kennungen, 105
Dateisysteme mounten
(Siehe Speicher, Dateisystem, mounten)
Daten
gemeinsamer Zugang zu, 136, 137
Globale Eigentumsfragen, 138
devlabel, 105
df Befehl, 110
Die Arbeitsmenge (Working Set), 58
Dokumentation
Red Hat Enterprise Linux-spezifische Informationen, 10
Dokumentation, Bedarf an, 2
Drucker
Duplex, 149
Erwägungen, 149
Farbe, 152
CMYK, 152
Laser, 153
Tintenstrahl, 152
Lokal, 155
Sprachen
(Siehe Seitenbeschreibungssprachen (Page Description Languages PDL))
Typen, 149
Anschlag, 151
Farblaser, 153
Farbstoffsublimation, 154
Laser, 153
Punktmatrix, 151
Thermalwax, 154
Tintenstrahl, 152
Typenrad, 151
Volltontinte, 154
Zeile, 151
Vernetzt, 155
verwalten, 149
Zusätzlich Quellen, 157
Druckerkonfiguration, 156
CUPS, 156
text-basierte Applikation, 156

E

Engineering, Social, 7
EXT2 Dateisystem, 106
EXT3-Dateisystem, 106

F

Farblaserdrucker, 153
Festplattenplatz
  (Siehe Speicher)
Festplattenquoten
  aktivieren, 118
  Einführung in, 116
  Verwaltung von, 119
  Überblick über, 116
    "Harte" Grenzen, 117
    "Weiche" Grenzen, 117
    Benutzer-spezifisch, 116
    Blocknutzung aufzeichnen, 117
    Dateisystem-spezifisch, 116
    Gnadenfristen, 117
    Gruppen-spezifisch, 116
    Inode-Nutzung aufzeichnen, 117
free-Befehl, 20, 61

G

Gerät
  Alternativen zu Gerätedateinamen, 104
  Benennen mit devlabel, 105
  Dateinamen, 103
  Dateisystemkennungen (Labels), 105
  devlabel, Benennen mit, 105
  Gerätenamen, Alternativen, 104
  Kennungen, Dateisystem, 105
  Namenskonvention, 102
  Partition, 103
  Typ, 103
  Unit, 103
  Zugriff zum Gesamt-Gerät, 104
Geschäft, Wissen über, 6
GID, 140
gnome-system-monitor-Befehl, 22
gpasswd-Befehl, 144
groupadd-Befehl, 144
groupdel-Befehl, 144
groupmod-Befehl, 144
grpck-Befehl, 144
Gruppe
  Berechtigungen bezogen auf, 139
    ausführen, 139
    lesen, 139
    schreiben, 139
    Setgid, 139
    Setuid, 139
    Sticky Bit, 139
  Dateien, die kontrollieren, 141
    /etc/group, 143
    /etc/gshadow, 144
    /etc/passwd, 141
    /etc/shadow, 142
  Gemeinsamer Datenzugriff mittels, 137
  GID, 140
  Struktur, festlegen, 137
  System-GIDs, 140
  System-UIDs, 140
  Tools zum Verwalten, 144
    gpasswd-Befehl, 144
    groupadd-Befehl, 144
    groupdel-Befehl, 144
    groupmod-Befehl, 144
    grpck-Befehl, 144
  UID, 140
  Verwaltung von, 125
Gruppen-ID
  (Siehe GID)

H

Hardware
  Ausfall der, 159
  Ersatzteile
    bereithalten, 159
    Bestand, Auswahl, 160
    Ersatzteile, Mengen, 160
    Tauschen von Hardware, 161
  Kompetenz für die Reparatur, 159
  Serviceverträge, 161
    Abzudeckende Hardware, 164
    Budget für, 164
    Depot-Service, 162
    Drop-Off Service, 162
    Reaktionszeit, 163
    Techniker vor-Ort, 163
    Verfügbarkeit von Teilen, 164
    Verfügungsstunden, 162
    Walk-In Service, 162
Heimverzeichnis
  zentralisiert, 138

I

IDE-Schnittstelle
  Überblick über, 73
Intrusion Detection Systeme, 10
iostat-Befehl, 24, 43
ISO 9660-Dateisystem, 106

K

Kapazitätsplanung, 16
Katastrophenvorbereitung, 159
  Arten von Katastrophen, 159
    Abstürze des Betriebssystems, 165
    Aufhängen des Betriebssystems, 166
    Ausfälle des Betriebssystems, 165
    Ausfälle von Applikationen, 166
    Bedienerfehler, 174
    Benutzerfehler, 174
    Elektrizität, 168
    Elektrizität, Qualität der, 169
    Fehler des Wartungspersonals, 177
    Fehler innerhalb von Prozessen, 175
    Fehler von Systemadministratoren, 175
    Gebäudeintegrität, 168
    Hardware-Ausfälle, 159
    Heizung, 173
    HLK, 173
    Klimaanlage, 173
    Konfigurationsfehler, 176
    Lüftung, 173
    Menschliches Versagen, 174
    Software-Ausfälle, 165
    Strom, Sicherheit im Umgang mit, 168
    Umgebungsbedingte Ausfälle, 168
    unsachgemäß bediente Applikationen, 174
    Unsachgemäße Reparaturen, 178
    Verfahrenstechnische Fehler, 175
    Wartungsbezogene Fehler, 177
    Wetter-bezogen, 173
  Strom, Backup, 170
    Generator, 172
    Motor-Generator-Satz, 171
    Stromausfälle, langfristig, 173
    USV (Unterbrechungsfreie Stromversorgung), 171
Kommunikation
  Notwendigkeit, 3
  Red Hat Enterprise Linux-spezifische Informationen, 10
Konventionen
  Dokument, ii

L

Laserdrucker, 153
  Farbe, 153
  Verbrauchsmaterialien, 154
Leseberechtigung, 139
Logical Volume Management (LVM)
  (Siehe LVM)
lpd, 157
LVM
  Datenmigration, 91
  in der Größe anpassen, logisches Volumen, 90
  Logisches Volumen in der Größe anpassen, 90
  Migration, Daten, 91
  Speichergruppierung, 90
  Vergleich zu RAID, 91
  Überblick über, 90

M

Missbrauch, Ressourcen, 138
Mount-Punkte
  (Siehe Speicher, Dateisystem, Mount-Punkt)
mpstat-Befehl, 24
MSDOS-Dateisystem, 107

N

NFS, 110

O

OProfile, 20, 28

P

PAM, 10
Partition, 103
  Attribute von, 79
    Geometrie, 79
    Typ, 79
    Typenfeld, 80
  Erstellen von, 100, 112
  erweitert, 79
  logisch, 80
  Primär, 79
  Überblick über, 78
passwd-Befehl, 144
Passwort, 128
  die Kürze von, 129
  Erinnerungswert, 132
  Fälligkeit, 133
  geschrieben, 131
  großer Zeichensatz benutzt in, 132
  kleiner Zeichensatz benutzt in, 130
  länger, 132
  mehrmals benutzt, 131
  Personliche Information benutzt in, 131
  schwach, 129
  stark, 132
  Wortspiele benutzt in, 131
  Wörter benutzt in, 130
Perl, Automatisierung und, 9
Philosophie der Systemadministration, 1
physikalischer Speicher

(Siehe Speicher)
Planen, Wichtigkeit von, 8
Plattenlaufwerke, 55
Pluggable Authentication Modules
(Siehe PAM)
printconf
(Siehe Druckerkonfiguration)
Printer Configuration Tool
(Siehe Druckerkonfiguration)
printtool
(Siehe Druckerkonfiguration)
Prozessleistung, Ressourcen bezogen auf
(Siehe Ressourcen, System, Prozessleistung)
Punktmatrixdrucker
(Siehe Anschlagdrucker)

Q

Quoten, Festplatte
(Siehe Festplattenquoten)

R

RAID
Arrays
Neu erstellen, 122
raidhotadd-Befehl, Verwendung, 122
Status, prüfen, 121
Verwaltung von, 121
Arrays erstellen
(Siehe RAID, Arrays, erstellen)
Arrays, erstellen, 119
Nach der Installation, 120
zum Installationszeitpunkt, 120
Einführung in, 84
Implementierungen von, 89
Hardware-RAID, 89
Software-RAID, 89
Levels von, 85
Nested RAID, 88
RAID 0, 85
RAID 0, Nachteile, 86
RAID 0, Vorteile von, 86
RAID 1, 86
RAID 1, Nachteile, 86
RAID 1, Vorteile, 86
RAID 5, 87
RAID 5, Nachteile, 88
RAID 5, Vorteile, 87
Nested RAID, 88
Vergleich zu LVM, 91
Überblick über, 85
raidhotadd-Befehl, Verwendung, 122
RAM, 54
Red Hat Enterprise Linux-spezifische Information
Ressourcenkontrolle
Speicher, 61
Tools zur Ressourcenkontrolle
free, 61
sar, 61
vmstat, 61
Tools zur Überwachung von Ressourcen
iostat, 43
sar, 44, 46
top, 44
vmstat, 42, 45
Überwachung von Ressourcen
Bandbreite, 42
CPU-Leistung, 42
Red Hat Enterprise Linux-spezifische Informationen
Automatisierung, 9
Backup-Technologien
AMANDA, 192
cpio, 191
dump, 191
tar, 190
Überblick über, 190
Bash Shell, 9
Dokumentation, 10
Intrusion Detection Systeme, 10
Kommunikation, 10
PAM, 10
Perl, 9
Ressourcenüberwachungstools, 20
free, 20
OProfile, 20
Sysstat, 20
top, 20
vmstat, 20
RPM, 10
Shell-Skripte, 9
Sicherheit, 10
Software-Support, 189
Support, Software, 189
Wiederherstellung nach einem Disaster, 189
Registrieren Ihres Abonnements, v
Rekursion
(Siehe Rekursion)
Ressourcen, System
Bandbreite, 35
Bussen, Beispiele von, 36
Busses Rolle in, 35
Datenpfade, Beispiele von, 36
Datenpfade, Rolle in, 36
Kapazität, erhöhen, 37
Last, reduzieren, 37
Last, verteilen, 37
Lösungen zu Problemen mit, 37
Probleme bezogen auf, 36
Überblick über, 35
Überwachung von, 18

Prozessleistung, 35
Applikationen, eliminieren, 40
Applikations-Overhead, reduzieren, 40
Applikationsbenutzung von, 39
Betriebssystem-Benutzung von, 39
Betriebssystem-Overhead, reduzieren, 40
CPU, upgraden, 41
Engpass, verbessern, 40
Fakten bezogen auf, 38
Kapazität, erhöhen, 41
Konsumenten von, 39
Last, reduzieren, 40
SMP, 41
Symmetrisches Multiprocessing, 41
Upgraden, 41
Überblick über, 38
Überwachung von, 17
Speicher
(Siehe Speicher)
Speicherplatz
(Siehe Speicherplatz)
Ressourcen, Wichtigkeit von, 6
Ressourcen-Missbrauch, 138
Ressourcenüberwachung, 15
Bandbreite, 18
Kapazitätsplanung, 16
Konzepte hinter, 15
Prozessorleistung, 17
Speicher, 19
Speicherplatz, 19
Systemleistung, 16
Tools
free, 20
GNOME System Monitor, 22
iostat, 24
mpstat, 24
OProfile, 28
sa1, 24
sa2, 24
sadc, 24
sar, 24, 27
Sysstat, 24
top, 21
vmstat, 23
Tools verwendet, 20
Was überwachen?, 16
Systemkapazität, 16
RPM, 10
RPM Paket Manager
(Siehe RPM)

S

sa1-Befehl, 24
sa2-Befehl, 24
sadc-Befehl, 24
sar-Befehl, 24, 27, 44, 46, 61
Reporte, lesen, 27
Schreibberechtigung, 139
SCSI-Festplatten
hinzufügen, 98
SCSI-Schnittstelle
Überblick über, 73
Seitenaustausch (Swapping), 59
Seitenbeschreibungssprachen (Page Description Languages PDL), 155
Interpress, 155
PCL, 155
PostScript, 155
Seitenfehler, 58
setgid-Berechtigung, 10, 139
Setuid-Berechtigung, 139
setuid-Berechtigungen, 10
Shell-Skripte, 9
Sicherheit
Red Hat Enterprise Linux-spezifische Informationen, 10
Wichtigkeit von, 7
SMB, 111
SMP, 41
Social Engineering, Risiken, 7
Software
Support für
Dokumentation, 166
E-Mail-Support, 167
Selbsthilfe, 166
Telefon-Support, 167
Vor-Ort-Support, 167
Web-Support, 167
Überblick, 166
Speicher
Datei-bezogene Probleme, 95
Datei-Sharing, 96
Dateizugang, 95
Dateisystem, 80, 105
/etc/mtab-Datei, 108
/proc/mounts-Datei, 109
Anzeige der Mounts, 108
datei-basiert, 80
df Befehl, verwenden, 110
Erstellungszeiten, 81
EXT2, 106
EXT3, 106
Haushaltung des Speicherplatzes, 82
Haushaltung, Speicherplatz, 82
Hierarchische Verzeichnisse, 81
ISO 9660, 106

Modifizierungszeiten, 81
Mount-Punkte, 107
Mounten, 107
Mounten mit der Datei /etc/fstab, 111
MSDOS, 107
Struktur, Verzeichnis, 82
Verzeichnisse, 81
VFAT, 107
Zugang ermöglichen zu, 83
Zugriffskontrolle, 81
Zugriffszeiten, 81
Einsatz, 78
Festplattenquoten, 94
(Siehe Festplattenquoten)
hinzufügen, 96, 112
/etc/fstab, aktualisieren, 114
ATA Festplatte, 97
Backup-Planung, ändern, 101
Formatieren, 100, 113
Hardware, installieren, 97
Konfiguration, aktualisieren, 100
Partitionieren, 100, 112
SCSI-Festplatten, 98
Löschen, 101, 114
/etc/fstab, entfernen von, 114
Daten, entfernen, 101
Inhalte löschen, 102, 115
umount Befehl, Verwendung, 114
Massen-Speicher-Geräte
Adressierung, Block-basiert, 71
Adressierung, Geometrie-basiert, 69
Adresskonzepte, 69
Befehlsverarbeitung, 76
Bewegung des Zugriffsarms, 76
Bewegung, Zugriffsarm, 76
Block-basierte Adressierung, 71
Disk Platten, 67
elektrische Einschränkungen von, 75
Geometrie, Probleme mit, 70
Geometrie-basierte Adressierung, 69
I/O-Lasten, Lesen, 77
I/O-Lasten, Performance, 77
I/O-Lasten, Schreiben, 77
I/O-Ort, 78
IDE-Schnittstelle, 73
Industrie-Standard-Schnittstellen, 72
Kopf, 70
Köpfe, 68
Köpfe lesen, 76
Köpfe schreiben, 76
Lesen versus Schreiben, 77
mechanische Einschränkungen von, 75
Performance von, 75
Platten, Disk, 67
Rotationsbedingte Latenz (Wartezeit), 76
Schnittstellen für, 71
Schnittstellen, Geschichte, 71
Schnittstellen, Industrie-Standard, 72
SCSI-Schnittstelle, 73
Sektor, 70
Verarbeitung, Befehl, 76
Wartezeit, rotationsbedingt, 76
Zugriffsarme, 68
Zylinder, 70
Überblick über, 67
netzwerk-zugänglich, 83, 110
NFS, 110
SMB, 111
Partition
Attribute von, 79
erweitert, 79
Geometrie von, 79
logisch, 80
Primär, 79
Typ von, 79
Typenfeld, 80
Überblick über, 78
RAID-basiert
(Siehe RAID)
Ressourcenverwendung von, 51
Technologien, 51
Cache-Speicher, 52
CPU-Register, 52
Datensicherungsspeicher (Backup-Speicher), 55
Festplatte, 55
Hauptspeicher, 54
L1-Cache, 53
L2-Cache, 53
Offline-Speicher, 55
Plattenlaufwerk, 55
RAM, 54
Technologien, fortgeschritten, 83
Verwaltung von, 67, 91
Ansteigen, normal, 94
Applikationsnutzung, 93
Benutzerangelegenheiten, 92
Übermäßige Nutzung von, 92
Überwachen freien Speicherplatzes, 91
virtueller Speicher, 56
Die Arbeitsmenge (Working Set), 58
Leistungsfähigkeit von, 59
Leistungsfähigkeit, bester Fall, 60
Leistungsfähigkeit, schlimmster Fall, 60
Seitenaustausch (Swapping), 59
Seitenfehler, 58
Virtueller Adressbereich, 57
Zusatzspeicher, 57
Überblick über, 56
Zugriffsmuster, 51
Überwachung von, 19
Speicherplatz
Überwachung von, 19

StickyBit-Berechtigung, 139
Symmetrisches Multiprocessing, 41
Sysstat, 20, 24
System Ressourcen
  (Siehe Ressourcen, System)
system-config-printer
  (Siehe Druckerkonfiguration)
Systemadministration
  Philosophie der, 1
    Automatisierung, 1
    Benutzer, 6
    Dokumentation, 2
    Geschäft, 6
    Kommunikation, 3
    Planen, 8
    Ressourcen, 6
    Sicherheit, 7
    Social Engineering, Risiken, 7
    Unerwartete Ereignisse, 8
Systemleistungskontrolle, 16

T

Tintenstrahldrucker, 152
  Verbrauchsmaterialien, 152
Tools
  Benutzer-Accounts, verwalten
    (Siehe Benutzer-Account, Tools zum Verwalten)
  Gruppen, verwalten
    (Siehe Gruppen, Tools zum Verwalten)
  Ressourcenüberwachung, 20
    free, 20
    GNOME System Monitor, 22
    iostat, 24
    mpstat, 24
    OProfile, 28
    sa1, 24
    sa2, 24
    sadc, 24
    sar, 24, 27
    Sysstat, 24
    top, 21
    vmstat, 23
top-Befehl, 20, 21, 44
Typenraddrucker
  (Siehe Anschlagdrucker)

U

UID, 140
useradd-Befehl, 144
userdel-Befehl, 144
usermod-Befehl, 144

V

verwalten
  Drucker, 149
VFAT-Dateisystem, 107
Virtueller Adressbereich, 57
virtueller Speicher
  (Siehe Speicher)
vmstat-Befehl, 20, 23, 42, 45, 61

W

watch-Befehl, 20
Wiederherstellung nach einem Disaster
  Backup-Ort, 187
    Belegschaft, 188
    Netzwerkverbindung, 188
  Einführung in, 185
  Ende, 189
  Hardwareverfügbarkeit, 188
  Plan, erstellen, testen, implementieren, 186
  Softwareverfügbarkeit, 188
  Verfügbarkeit von Backups, 188

Z

Zeilendrucker
  (Siehe Anschlagdrucker)
zentralisiertes Heimverzeichnis, 138

Colophon

Die Handbücher wurden im Format DocBook SGML v4.1 erstellt. Die HTML- und PDF-Formate werden unter Verwendung benutzerdefinierter DSSSL Stylesheets und benutzerdefinierten Jade Wrapper Scripts angelegt. Die DocBook SGML-Dateien wurden in **Emacs** mithilfe von PSGML Mode geschrieben.

Garrett LeSage schuf das Design der Grafiken für Meldungen (Anmerkung, Tipp, Wichtig, Achtung und Warnung). Diese dürfen frei zusammen mit der Red Hat-Dokumentation vertrieben werden.

Das Team der Red Hat-Produktdokumentation besteht aus:

Sandra A. Moore — Verantwortliche Autorin/Bearbeiterin des *Red Hat Enterprise Linux Installationshandbuch für x86, Itanium™, AMD64 und Intel® Extended Memory 64 Technology (Intel® EM64T)* Verantwortliche Autorin/Bearbeiterin des *Red Hat Enterprise Linux Installationshandbuch für IBM® S/390® und IBM® eServer™ zSeries® Architekturen* Verantwortliche Autorin/Bearbeiterin des *Red Hat Enterprise Linux Installationshandbuch für IBM® POWER Architecture Architekturen*

John Ha — Verantwortlicher Autor/Bearbeiter des *Red Hat Cluster Suite Configuring and Managing a Cluster*; Co-Autor/Co-Bearbeiter des *Red Hat Enterprise Linux Sicherheitshandbuch*; Bearbeiter von custom DocBook-Stylesheets und Skripts

Edward C. Bailey — Verantwortlicher Autor/Bearbeiter des *Red Hat Enterprise Linux Einführung in die System-Administration*; Verantwortlicher Autor/Bearbeiter der *Release Notes*; Co-Autor des *Red Hat Enterprise Linux Installationshandbuch für x86, Itanium™, AMD64 und Intel® Extended Memory 64 Technology (Intel® EM64T)*

Karsten Wade — Verantwortlicher Autor/Bearbeiter des *Red Hat SELinux Application Development Guide*; Verantwortlicher Autor/Bearbeiter des *Red Hat SELinux Policy Writing Guide*

Andrius Benokraitis — Verantwortlicher Autor/Bearbeiter des *Red Hat Enterprise Linux Referenzhandbuch*; Co-Autor/Co-Bearbeiter des *Red Hat Enterprise Linux Sicherheitshandbuch*; Co-Autor des *Red Hat Enterprise Linux Handbuch zur System-Administration*

Paul Kennedy — Verantwortlicher Autor/Bearbeiter des *Red Hat GFS Administrator's Guide*; Co-Autor des *Red Hat Cluster Suite Configuring and Managing a Cluster*

Mark Johnson — Verantwortlicher Autor/Bearbeiter des *Red Hat Enterprise Linux Desktop Configuration and Administration Guide*

Melissa Goldin — Verantwortlicher Autor/Bearbeiter des *Red Hat Enterprise Linux Schrittweise Einführung*

Das Red Hat-Team verantwortlich für Übersetzungen besteht aus:

Amanpreet Singh Alam — Technische Übersetzung - Punjabi

Jean-Paul Aubry — Technische Übersetzung - Französisch

David Barzilay — Technische Übersetzung - Portugiesisch (Brasilien)

Runa Bhattacharjee — Technische Übersetzung - Bengali

Chester Cheng — Technische Übersetzung - Traditionelles Chinesisch

Verena Fuehrer — Technische Übersetzung - Deutsch

Kiyoto Hashida — Technische Übersetzung - Japanisch

N. Jayaradha — Technische Übersetzung - Tamil

Michelle Jiyeen Kim — Technische Übersetzung - Koreanisch

Yelitza Louze — Technische Übersetzung - Spanisch

Noriko Mizumoto — Technische Übersetzung - Japanisch

Ankitkumar Rameshchandra Patel — Technische Übersetzung - Gujarati

Rajesh Ranjan — Technische Übersetzung - Hindi
Nadine Richter — Technische Übersetzung - Deutsch
Audrey Simons — Technische Übersetzung - Französisch
Francesco Valente — Technische Übersetzung - Italienisch
Sarah Wang — Technische Übersetzung - Vereinfachtes Chinesisch
Ben Hung-Pin Wu — Technische Übersetzung - Traditionelles Chinesisch